(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 847 174**

(51) Int. CI.:

H04M 3/22 (2006.01)
H04M 3/436 (2006.01)
H04L 29/06 (2006.01)
H04M 7/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.08.2017 PCT/US2017/045090**

(87) Fecha y número de publicación internacional: **08.02.2018 WO18026912**

(96) Fecha de presentación y número de la solicitud europea: **02.08.2017 E 17752229 (9)**

(97) Fecha y número de publicación de la concesión europea: **25.11.2020 EP 3494690**

(54) Título: **Método y aparato para la identificación de amenazas mediante análisis de señalización de comunicaciones, eventos y participantes**

(30) Prioridad:

02.08.2016 US 201662370105 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.08.2021

(73) Titular/es:

PINDROP SECURITY, INC. (100.0%)
817 W. Peachtree St., NW, Suite 770
Atlanta, GA 30308, US

(72) Inventor/es:

DOUGLAS, LANCE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y aparato para la identificación de amenazas mediante análisis de señalización de comunicaciones, eventos y participantes

Antecedentes

Los eventos de señalización y corroboración de la red de comunicaciones pueden proporcionar, y/o ser interrogados para aislar, indicadores de la naturaleza compleja de una llamada telefónica, la persona que llama y/o la intención de la persona que llama. Supervisando la señalización, se puede determinar la autenticidad de un intento de llamada telefónica.

Los documentos WO 2010/025805 y US 2007/150773 representan ejemplos de sistemas de la técnica anterior para la detección de llamadas de amenazas.

Resumen

Esta especificación describe tecnologías relacionadas con la detección o identificación de llamadas telefónicas, personas que llaman o dispositivos que pueden considerarse una amenaza. Más específicamente, los aspectos de la presente descripción se relacionan con la identificación de amenazas mediante el análisis de la señalización de comunicaciones, eventos y participantes, especialmente con respecto a las redes telefónicas.

En general, un aspecto del tema descrito en esta especificación se puede realizar en un método o aparato ejecutado por ordenador.

Los aspectos de la invención incluyen un método para determinar una puntaje de amenaza de una llamada que atraviesa una red de telecomunicaciones, según las reivindicaciones 1 y 6.

Las reivindicaciones dependientes 2-5, 7 y 8 proporcionan aspectos adicionales.

Los aspectos de la invención incluyen una plataforma de aplicaciones de redes de telecomunicaciones, según las reivindicaciones 9 y 13.

Las reivindicaciones dependientes 10-12, 14 y 15 proporcionan aspectos adicionales.

Los detalles de uno o más ejemplos se exponen en los dibujos adjuntos que se dan sólo a modo de ilustración, conla descripción a continuación. Otras características, aspectos y ventajas de la invención resultarán evidentes a partir de la descripción, los dibujos y las reivindicaciones. Los números de referencia y las designaciones similares en los diversos dibujos indican elementos similares. El alcance de la protección está definido por las reivindicaciones adjuntas.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques que ilustra la ruta de una llamada telefónica según la tecnología convencional.

La figura 2 es un diagrama de bloques que ilustra una ruta de una llamada telefónica que incluye una plataforma de aplicación de red inteligente de acuerdo con un ejemplo.

La figura 3 es un diagrama de bloques que ilustra una ruta de una llamada telefónica que incluye instalaciones seguras de red inteligente de próxima generación de acuerdo con uno o más ejemplos.

La figura 4 es un diagrama de bloques que ilustra una plataforma de aplicación de red inteligente y una ruta de una llamada telefónica de acuerdo con uno o más ejemplos.

La figura 5 es un diagrama que ilustra una parte de un flujo de llamadas según uno o más ejemplos. La figura 5 puede leerse junto con la figura 7 o la figura 8.

La figura 6 es un diagrama de bloques que ilustra un dispositivo de ordenadorde ejemplo que puede utilizarse para realizar parte de varios otros ejemplos.

La figura 7 es un diagrama que ilustra una parte de un flujo de llamadas según uno o más ejemplos. La figura 7 puede leerse junto con la figura 5 y como alternativa a la figura 8.

La figura 8 es un diagrama que ilustra una parte de un flujo de llamadas según uno o más ejemplos. La figura 8 puede leerse junto con la figura 5 y como alternativa a la figura 7.

La figura 9 es un diagrama que ilustra un flujo de llamadas que incluye una función de bifurcación y una función de grabación de llamadas según uno o más ejemplos.

La figura 10 es un diagrama que ilustra un flujo de llamadas en el que la llamada no se encamina a una función de

bifurcación según uno o más ejemplos.

La figura 11a, 11b, 11c y 11d son diagramas de bloques que ilustran métodos para la identificación de amenazas a través del análisis de la señalización de comunicaciones, eventos y/o participantes.

La figura 12 es un diagrama de bloques que ilustra un método para etiquetar una llamada con un identificador de correlación tanto en el extremo de origen como en el de terminación de la llamada de acuerdo con uno o más ejemplos.

Descripción detallada

La señalización telefónica ha evolucionado durante los últimos cuarenta años y se relaciona específicamente con la intercomunicación entre los sistemas responsables de habilitar, encaminar y supervisar las llamadas telefónicas locales e internacionales. Esta señalización comenzó como tonos audibles enviados junto con los medios de voz (señalización en banda) y se ha separado casi por completo de la parte audible de una llamada (señalización fuera de banda).

Existen varias recomendaciones formales de señalización, denominadas libremente normas, que definen la estructura, el contenido y los interfaces del mensaje en las que los sistemas de señalización pueden confiar para funcionar correctamente dentro de las redes de comunicaciones globales. Principalmente, los dos conjuntos de recomendaciones que se utilizan en la actualidad son de la serie Q.700 de ITU-T, a nivel mundial, y según lo normalizado por ANSI en Norteamérica. La señalización en fijo/fijo y móvil es similar, y la señalización móvil tiene una mejor normalización a nivel mundial ya que la interoperabilidad para tránsito y facturación fue primordial para su madurez.

Según la serie ITU-T Q.1200 (redes fijas-INAP CS2) y CAMEL (redes móviles-CAP), la señalización de comunicaciones puede encaminarse a un punto de control de servicio (SCP) desde el punto de conmutación de servicio (SSP) o móvil o desde el Centro de Conmutación (MSC), mientras que el SSP/MSC son los nodos de instalaciones de telefonía inicial (de origen) y final (de terminación) responsables de habilitar una llamada telefónica. Debido a la complejidad de la miríada de realizaciones de normas de red en los sistemas de línea fija, la señalización se basa en un traspaso de un nodo de red al siguiente en el camino hacia el SSP/MSC de destino predefinido, sin tener en cuenta ciertos conocimientos. sobre los nodos participantes anteriores o pendientes.

Este enfoque de salto de nodo es excelente para permitir que redes dispares funcionen de forma independiente para que una llamada atraviese de manera cooperativa sus redes, independientemente del participante de red anterior y de cualquier red participante pendiente. Sin embargo, este salto de nodo también permite ofuscar la identidad de la persona que llama debido a la falta de un origen verdadero, o de una ruta total tomada, estando la información disponible; falta de verificación de autorización de la información proporcionada por la parte que llama (por ejemplo, el número de teléfono de la persona que llama no está validado para el uso autorizado por la parte que llama o su dispositivo); y falta de fiabilidad de que cualquier información de validación proporcionada en la señalización, en cualquier punto de la llamada, no será eliminada o manipulada por ningún otro punto de la llamada antes del SSP/MSC de destino.

Dado que la facturación es la función empresarial central que realizan todas las redes, el aspecto más maduro de las redes de señalización es la integración de facturación en el origen de la llamada y servicios similares como el redireccionamiento (por ejemplo, números de teléfono gratuito 800, correo de voz). Además, las redes móviles, debido a la naturaleza transeúnte de los dispositivos utilizados para exponer a los abonados facturables a los servicios de red, han tenido la oportunidad de ser significativamente más maduros en las áreas de control de facturación y la normalización de la interoperabilidad de facturación.

Si bien los sistemas de facturación de cada red pueden ser las funciones más maduras, generalmente son los menos expuestos a otras redes para interrogación, corroboración o colaboración con respecto a la validez de la información proporcionada o no proporcionada en los mensajes de señalización de llamadas. Por lo tanto, existe un potencial real de que existan amenazas de partes que pueden esconderse detrás de redes que han sido víctimas del origen no autorizado de una llamada con datos falsos o que se sabe que eliminan información de identificación cuando se utilizan como una de las potencialmente cientos de nodos participantes para entregar una llamada telefónica a su destino.

En un ejemplo, los detalles y las estadísticas sobre el SSP/MSC utilizados para originar la llamada (también conocidos como "datos del borde exterior) se comparan con datos históricos o de terceros en tiempo real, para determinar la propensión de las llamadas que se originan en esas instalaciones a ser categorizada como una amenaza. El almacenamiento de los datos del borde exterior antes de que se envíe la llamada a través de la red de comunicaciones permite que dichos datos se conserven y no estén sujetos a manipulaciones durante el recorrido de la red de comunicaciones. Esto permite la identificación de intentos de amenazas basados en los datos del borde exterior de instalaciones de origen, permitiendo así el aislamiento de una instalación de red comprometida que puede o no ser conocida por su respectivo propietario de red. El resultado de esta realización permite tomar varias acciones como las siguientes: protección de las partes llamadas y amenazas potenciales antes de que la llamada termine dentro de su red; informar a los propietarios de la red de las instalaciones de red comprometidas; la información de las fuerzas del orden y los organismos reguladores de la actividad de amenazas; y/o el aislamiento del tráfico de red que se origina en una instalación de red comprometida para enriquecer aún más las capacidades de detección de amenazas. Otras

acciones que se pueden tomar incluyen acciones dinámicas o predeterminadas tales como redirigir la llamada telefónica a un nuevo destino, como un agente altamente calificado, un sistema IVR/VRU para autenticación automatizada o correo de voz; dividir el audio en una instalación de grabación, supervisión o escucha; y/o colgar a la persona que llama.

En otro ejemplo, el análisis de la varianza (ANOVA) de la precisión de los detalles de la persona que llama y su dispositivo desde las perspectivas del SSP/MSC utilizado para originar la llamada y el SSP/MSC utilizado para terminar la llamada se comparan para identificar el potencial de amenaza. Esto permite la identificación de la varianza entre los datos suministrados desde las instalaciones de la red de origen menos fiables y las instalaciones de la red de terminación potencialmente más fiables. Por medio de esta varianza, se puede determinar que la información se proporcionó incorrectamente a través de la red de origen y/o se modificó o eliminó mientras estaba en tránsito hacia la red de terminación. Con un interrogatorio adicional de los sistemas de los propietarios de la red, las bases de datos de los reguladores y/o los sistemas de datos, las varianzas maliciosas pueden aislarse de las benignas.

En otro ejemplo, el Identificador Internacional de Equipo Móvil (IMEI), o identificador de equipo, se rastrea a través de las llamadas y se compara en tiempo real, o después de la llamada, con datos de terceros para determinar los niveles de amenaza. Al rastrear los dispositivos utilizados en llamadas dispares y sistemas de terceros, se puede evaluar la validez de la información proporcionada con respecto al dispositivo de la persona que llama. Con esta información, se puede determinar la información estadística sobre el uso del dispositivo, y se pueden identificar valores atípicos como la hora del día, repetición de llamadas, anomalías de ubicación y estado de propiedad, lo que permite proteger de amenazas a las partes a las que se llama y a quienes llaman. intentos realizados en los dispositivos de este último o en su nombre. Además, al conocer el tipo de dispositivo, los sistemas internos y de terceros pueden ser interrogados adicionalmente en busca de datos relevantes que puedan compararse con ese tipo de dispositivo.

En otro ejemplo, el Identificador Internacional de Abonado Móvil (IMSI), o identificador de abonado, se rastrea a través de las llamadas y se valida con el presunto operador responsable. Esta información puede ser solicitada por redes fiables. Al conocer la identificador de abonado único, los sistemas internos y de terceros pueden ser interrogados para obtener información de corroboración relevante con respecto a la precisión de los datos proporcionados en la llamada tanto por la señalización como por la persona que llama. Por ejemplo, los datos de señalización pueden indicar que la llamada se origina en un MSC que está sirviendo estaciones base en el noreste de Atlanta, Georgia, pero el IMSI se usa para interrogar a la red del operador del abonado para determinar que el abonado no está actualmente en la llamada y está conectado a un MSC que presta servicios a estaciones base en Reno, Nevada; con esta información expuesta al agente del centro de llamadas, al que se dirige la llamada telefónica, el agente puede ver la información contradictoria y preguntar casualmente a la persona que llama desde dónde está llamando para determinar la corroboración o una varianza adicional, y actuar en consecuencia.

En otra realización de la invención, se puede rastrear una combinación de IMEI e IMSI para aislar los intentos de ofuscación de una llamada por un abonado y/o dispositivo de una llamada válida por ese mismo abonado o dispositivo, permitiendo la verdadera identificación de al menos un participante en un intento de amenaza. Con estos dos datos disponibles para algunas o todas las llamadas supervisadas como se describe en este documento, la información interna y de terceros en tiempo real, histórica y de autenticación de llamadas se puede utilizar para determinar si el dispositivo y/o el abonado es parte de un grupo organizado que perpetra amenazas. Por ejemplo, se pueden usar muchos "teléfonos quemadores" durante un ataque organizado contra víctimas a través de múltiples canales, como correo electrónico, teléfono, chat y mensajería social. Al recopilar y analizar esta combinación de datos cuando esté disponible, se pueden identificar tanto los anillos de fraude nuevos como los crecientes, así como los falsos positivos. Un buen ejemplo es el caso en el que un teléfono de grabación se utiliza varias veces pero con nuevas tarjetas de módulo de identificación de abonado (SIM). Se puede determinar que para un intento de amenaza confirmado, cada tarjeta SIM que se usó en el dispositivo es sospechosa, al igual que cualquier dispositivo futuro en el que se use la tarjeta SIM. Además, cualquier apariencia de una utilización "válida" de cualquier parte de una combinación sospechosa en cualquier momento entre intentos de amenaza de IMEI e IMSI no coincidentes puede ser supervisada, para descubrir la identidad real del propietario de una tarjeta SIM en posesión de un dispositivo sospechoso de fraude, o viceversa.

Los sistemas y métodos descritos en este documento se pueden usar durante las partes restantes de la llamada para detectar más a fondo la supuesta amenaza y se puede recopilar información adicional. Además, pueden estar involucrados los medios de comunicación o las fuerzas del orden.

Se puede utilizar la funcionalidad SCP personalizada para gestionar el control total de la señalización de una parte de la llamada. El dispositivo, el abonado, el contenido y/o los eventos de terceros pueden analizarse para determinar el potencial de identificación de amenazas de múltiples llamadas.

El control de señalización puede encaminarse a un sistema de control de señalización dinámico durante el establecimiento de la llamada, antes de que cualquiera de las partes escuche el timbre. El control de señalización puede usarse para autenticar, autorizar y supervisar tanto la señalización de comunicaciones como los medios para proporcionar cualquiera de los siguientes: servicios de facturación mejorados, junto con la invención explicada; validación de la información suministrada en una única llamada para evaluar la posibilidad de una llamada maliciosa; y/o análisis de los patrones y la información suministrada a través de múltiples llamadas dispares - y eventos no

derivados de la llamada - desde múltiples puntos en la llamada más allá del simple establecimiento de la llamada.

La figura 1 es un diagrama que ilustra una ruta 100 de una llamada telefónica típica en la técnica convencional. La parte que llama 110 realiza una llamada que es manejada por la central local 115. La llamada luego llega a una central de tránsito 120 y pasa a través de la red de tránsito 125. Hacia el extremo final de la ruta de la llamada, la llamada procede a la central de tránsito 130 y luego a la central local 135. Finalmente, la llamada llega a la parte llamada 140.

La figura 2 es un diagrama que ilustra una ruta 200 de una llamada telefónica, en la que la ruta incluye una plataforma de aplicación de red inteligente 250 de acuerdo con una o más realizaciones de la presente invención. La parte que llama 210 coloca una llamada que es manejada por la central local 215 en el extremo de origen. La central local 215 envía un disparador a la plataforma de aplicación de red inteligente 250 y encamina la llamada a la central de tránsito 220. La llamada pasa entonces a través de la red de tránsito 225 a la central de tránsito 230 y luego a la central local 235 en el extremo de terminación. El intercambio local 235 envía un disparador a la plataforma de aplicación de red inteligente 250 y encamina la llamada a la parte llamada 240. Mientras tanto, la plataforma de aplicación de red inteligente 250 intercambia información con la parte llamada 240.

La figura 3 es un diagrama que ilustra una ruta de una llamada telefónica que incluye instalaciones seguras de red inteligente de próxima generación (NGIN) 320 de acuerdo con uno o más ejemplos. La figura 3 incluye un teléfono 310, instalaciones de señalización de la portadora 315 en el lado de origen de la llamada, instalaciones de red inteligente segura de próxima generación (NGIN) 320, instalaciones de voz de la portadora 325 en el lado de origen de la llamada, sistema de señalización 7 (SS7)/transporte de señalización (SIGTRAN) red 330, instalaciones de señalización de la portadora 335 en el lado de terminación de la llamada, instalaciones de voz de la portadora 340 en el lado de terminación de la llamada, instalaciones de voz de NGIN 345, instalaciones de voz de cliente 350 y centro de llamadas de cliente empresarial 355.

Si bien el teléfono 310 se representa como un teléfono inteligente, las realizaciones no se limitan al mismo. Por ejemplo y sin limitación, el teléfono 310 podría ser un teléfono de marcación rotativa, un teléfono de marcación por tonos, un teléfono de línea fija, un teléfono celular, un protocolo de voz sobre Internet (teléfono VoIP) o un teléfono por software. Además, el teléfono 310 podría ser cualquier tipo de teléfono, incluidos aquellos capaces de producir tonos de señalización multifrecuencia de dos tonos (DTMF).

A continuación, se expondrá una ruta de llamada de ejemplo que implica instalaciones 320 seguras de NGIN de acuerdo con una o más realizaciones de la presente invención. Un número marcado 361 se marca en un teléfono 310. Las instalaciones de señalización del operador 315 en el lado de origen de la llamada envían una solicitud de activación 362 a las instalaciones de NGIN seguras 320. En respuesta al disparador 362, las instalaciones de NGIN seguras 320 almacenan los datos de borde exterior del llamante 363. Los datos de borde exterior del llamante pueden comprender señalización de conexión y/o metadatos, y la señalización de conexión y/o metadatos puede incluir información de determinación de identidad. La señalización de conexión incluye todo lo proporcionado desde la SSF/SSP hasta la SCF/SCP, los metadatos incluyen elementos específicos dentro de esa señalización que se refieren a otra información que requiere información relativa en otros sistemas para la adquisición de datos adicionales.

Por ejemplo, la SSF/SSP puede proporcionar un número de ubicación y un tipo de terminal, ambos que no son necesarios para la señalización de conexión de un extremo a otro, y el número de ubicación es específico para una combinación de proveedor de servicio y tipo de terminal, lo que significa que será necesario realizar una búsqueda en un recurso proporcionado por el proveedor de servicios para correlacionar esos datos con información útil.

Los datos de borde exterior de ejemplo incluyen lo siguiente:

CalledPartyNumber

CallingPartyBusinessGroupID

CallingPartySubaddress

FacilityGroup

FacilityGroupMember

OriginalCalledPartyID

Dígits

RedirectingPartyID

RedirectionInformation

RouteList

TravellingClassMark

Extensions

FeatureCode

AccessCode

Carrier

ComponentType

Component

ComponentCorrelationID

ServiceAddressInformation

LocationNumber

TerminalType

Extensions

USIServiceIndicator

USIInformation

CUApplicationInd

HighLayerCompatibility

PortadorCapability

GenericNumbers

A continuación, las instalaciones 320 seguras de NGIN envían un mensaje de reanudación 364 a las instalaciones 315 de señalización de la portadora en el lado de origen, que luego envían un mensaje a las instalaciones 325 de voz de la portadora en el lado de origen para encaminar la llamada 365 como de costumbre. Las instalaciones de voz en la portadora 325 en el lado de origen luego conectan la función de voz 366 al teléfono 310, haciendo que la persona que llama escuche el timbre del teléfono 310.

A continuación, la señalización de llamada atraviesa 367 la red SS7 hasta las instalaciones del anfitrión de DialedNumber, y los medios de llamada atraviesan 368 una red digital de servicios integrados (ISDN) hasta las instalaciones del host de DialedNumber. Una vez que la señalización de llamada ha llegado a las instalaciones de señalización de la portadora 335 en el lado de terminación de la llamada, las instalaciones de señalización de la portadora 335 envían una solicitud de activación 369 a las instalaciones de NGIN seguras 320, que almacenan los detalles 370 del borde interno de la persona que llama.

Los detalles del borde interno pueden incluir algunos o todos los datos del borde externo relacionados con la conectividad (por ejemplo, la parte llamada original, si es capaz de reenviar y se mantienen los datos, dirección de la parte que llama, ubicación), pero solo una dirección de la parte llamada se garantiza que se proporcionará, y no necesariamente la dirección original de la parte llamada. La varianza, en sí misma, es un método de indicación de información en el modelado y análisis inventivo.

Las instalaciones 320 seguras de NGIN instruyen entonces la unión de llamadas y/o la supervisión de eventos mediante el mensaje 371 a las instalaciones 335 de señalización de la portadora en el lado de terminación. Las instalaciones de señalización de la portadora 335 en el lado de terminación envían entonces un mensaje 372 a las instalaciones de voz de la portadora 340 en el lado de terminación para encaminar la llamada como de costumbre y unirse a la llamada a las instalaciones de voz NGIN 345. Las instalaciones de voz de la portadora 340 en el lado de terminación luego encaminan 373 el tráfico de voz tanto al equipo de las instalaciones del cliente (CPE) como a las instalaciones NGIN seguras 320. Se establecen comunicaciones 374 bidireccionales entre las instalaciones NGIN seguras 320 y el centro de atención telefónica del cliente 355. El operador puede enviar actualizaciones 375 de eventos opcionales instalaciones de señalización 335 en el lado de terminación a las instalaciones de NGIN seguras 320, que luego almacena o toma la acción 376 sobre las actualizaciones de eventos opcionales. Las instalaciones de voz del cliente 350 en el lado de terminación indican 377 el centro de llamadas de clientes empresariales 355 para manejar las llamadas aseguradas por las instalaciones de NGIN seguras 320. Las instalaciones de NGIN seguras 320 llenan los datos de puntaje en tiempo real 378 al centro de llamadas de clientes de la empresa 355.

La figura 4 es un diagrama que ilustra una plataforma de aplicación de red inteligente y una ruta de una llamada telefónica de acuerdo con uno o más ejemplos.

Incluida en la figura 4 hayuna plataforma de aplicación de red inteligente 450 que comprende un punto de transferencia de señal (STP) 420 en el lado de origen de la llamada, un punto de conmutación de servicio (SSP) 425 en el lado de origen de la llamada, un punto de control de servicio (SCP) 435, un STP 440 en el lado de terminación de la llamada y un SSP 445 en el lado de terminación de la llamada.

Los medios de llamada y el tráfico de señalización proceden de las fuentes de origen 410 a las instalaciones de origen 415. Tanto las fuentes de origen 410 como las instalaciones de origen 415 pueden no ser fiables. El tráfico de medios de llamada procede entonces desde las instalaciones de origen 415 al SSP 425 en el lado de origen de la llamada. El tráfico de señalización de llamada procede de las instalaciones de origen 415 a la plataforma de aplicación de red inteligente 450, donde el STP 420 puede recibir el tráfico de señalización de llamada. El STP 420 encamina el tráfico de señalización entre el SCP 435 y el SSP 425 en el lado de origen. El SCP 435 y el SSP 425 en el lado de origen pueden intercambiar mensajes directamente. El STP 420 puede encaminar el tráfico de señalización hacia y desde las instalaciones de origen 415.

La plataforma de aplicación de red inteligente 450 encamina el tráfico de medios de llamada a un servicio de tarifa premium (PRS) 430. El PRS 430 intercambia tráfico de señalización con la plataforma de aplicación de red inteligente 450. El PRS puede tener un interfaz especificado en el estilo de transferencia de estado representativo (REST); funcionalidad para registrar una sesión de Protocolo de inicio de Sesión (SIP) (SIP-REC); y/o lógica para recibir y enviar paquetes y códec (s) del Protocolo de Transporte en Tiempo Real (RTP) para el contenido de los paquetes RTP.

El tráfico de medios de llamada procede del SSP 425 en el lado de origen al SSP 445 en el lado de terminación. El SSP 445 en el lado de terminación puede intercambiar tráfico de señalización con el SCP 435. Un STP 440 en el lado de terminación puede encaminar tráfico de señalización entre el SSP 445 y el SCP 435. Las instalaciones de terminación 455 intercambian tráfico de señalización con la plataforma de aplicación de red inteligente 450. El STP 440 puede encaminar tráfico de señalización hacia y desde las instalaciones de terminación 455. El tráfico de medios de llamada procede del SSP 445 a las instalaciones de terminación 455 y luego a las instalaciones de cliente 460. Las instalaciones de terminación 455 y las instalaciones de cliente 460 intercambian tráfico de señalización. Las instalaciones de terminación 455 y las instalaciones del cliente 460 pueden ser fiables.

Los SSP 425 y 445 pueden tener un interfaz para protocolos de señalización SS7 / ISDN / SIGTRAN, SIP y RTP, y/o Protocolo de Control de Pasarela de Medios (MGCP). Los SSP 425 y 445 pueden realizarse en una oficina central/centralita local, como equipo en las instalaciones del cliente o como parte de las instalaciones 320 seguras de NGIN.

Los STP 420 y 440 pueden tener un interfaz para Aplicaciones Personalizadas para Lógica Mejorada para Redes Móviles (CAMEL) fase 2 o superior y/o Protocolo de Aplicación de Red Inteligente (INAP). Los STP 420 y 440 se pueden realizar como parte de las instalaciones 320 seguras de NGIN.

Además del temade la figura 4 descrito hasta ahora, el enlace troncal preexistente entre las instalaciones de origen 415 y las instalaciones de terminación 455 puede ser una ruta redundante 465 tomada por señalización y/o tráfico de medios.

La figura 5 es un diagrama que ilustra una parte de un flujo de llamadas según uno o más ejemplos. La figura 5 puede leerse junto con la figura 7 o la figura 8.

La figura 5 incluye la parte llamante 505, controlador de borde de sesión (SBC) 510, pasarela de medios (MGW) 515, MGW 520 y SCP 525. El SBC 510 puede ser un MSC o SSP de origen, dependiendo de la naturaleza de la llamada. Los MGW 515 y 520 pueden ser el mismo equipo o un equipo similar y pueden realizarse en forma de Pasarelas Serie Universal AS5400 de Cisco. Los MGW 515 y 520 pueden tener una conexión de parte de usuario ISDN (ISUP) contiguo a través de un STP.

Lo siguiente es una descripción de un ejemplo de flujo de llamadas según una o más realizaciones de la presente invención. Son posibles otros flujos de llamadas. El teléfono de la parte que llama 505 envía una solicitud SIP INVITE 530 al SBC 510 que incluye la parte/cliente que llama (CLI (Identificación de Línea de Llamada)) en un campo de encabezado De y el número de teléfono 705/805 del centro de llamadas en un campo de encabezado A.

En el caso de que el teléfono 505 de la parte que llama sea un teléfono móvil, el SBC 510 envía una solicitud 533 de la Parte de la Aplicación CAMEL (CAP) que tiene, por ejemplo y sin limitación, el contexto de la aplicación (AC) del servicio del Sistema Global para Comunicaciones con Móviles (GSM) función de conmutación (SSF) a función de control de servicio GSM (SCF) y punto de detección inicial (IDP) con los parámetros relevantes. Los parámetros de IDP relevantes de ejemplo pueden incluir, entre otros, los siguientes: SKI (ServiceKeyN (donde n es un id arbitrario pero específico de la realización; con más detalle, este parámetro se usa cuando se comunica con un SCF/SCP y ServiceKeyNumber es simplemente una identificación para correlacionar lo que el SSF/SSP pide al SSF/SCP que realice), el número de la parte llamante (CgPN), CdPBCDN (número decimal codificado en binario de la parte Llamada, dígitos marcados originalmente antes de la Desviación de la Llamada)) y BCSM DP (punto de detección), incluidos parámetros como información recopilada, CallRefN (un identificador único para la llamada; este parámetro proporciona el número de referencia de la llamada de red asignado a la llamada por el GMSC/MSC), el registro de ubicación de

visitantes (VLR), CellID (marcador de ubicación del área celular/torre a la que está conectado el dispositivo de la persona que llama (IMEI)), CID (un ID de Célula GSM (CID) es un número generalmente único que se utiliza para identificar cada estación transceptora base (BTS) o sector de un BTS dentro de un código de área de ubicación (LAC)) si no está dentro de una red GSM.)) MSC, IMSI y hora y zona horaria.

Al recibir la solicitud CAP 533, SCP 525 toma la acción 536 de la siguiente manera. Se crean un prefijo de encaminamiento para SSP-B y un identificador de correlación (ID). Más detalladamente, SSP-B es el SSP de borde interno (el que responde a la llamada). El SSP-A envía la señalización de la llamada al NGIN 320 y el NGIN 320 redirige la llamada cambiando la parte llamada, o actualiza el número de la parte que llama a un número único en el tiempo, de modo que cuando el NGIN 320 se consulte posteriormente en la mitad de la red o en SSP-B, los cambios actúan como identificadores únicos para esa llamada y se pueden analizar todos los demás datos internos/externos. Se establece una dirección de encaminamiento de destino DRA1 que comprende el prefijo de encaminamiento SSP-B, un prefijo de encaminamiento para SCP y un ID de correlación para la llamada. Los datos de los detalles de la llamada se asignan al ID de correlación y se almacenan. SCP 525 luego envía un mensaje CON 539 con un parámetro de DRA1.

SBC 510 envía una solicitud SIP INVITE 542 con el parámetro DRA1 a MGW 515 que envía un mensaje de dirección inicial de ISUP (IAM) 545 con los parámetros DRA1 y el número de la parte llamante a MGW 520. MGW 520 responde a MGW 515 con mensaje de dirección ISUP completa (ACM) 548 y, posteriormente, mensaje de respuesta ISUP (ANM) 551. MGW 515 envía códigos de respuesta SIP (número de referencia 554) 100, 180 o 183, según corresponda, y finalmente SIP 200 OK (número de referencia 557), al SBC 510. SBC 510 envía el código de respuesta SIP 200 OK 560 al teléfono 505 de la persona que llama. Al final de la llamada 505 de la parte que llama, el teléfono 505 de la parte que llama envía una solicitud SIP BYE 563 a SBC 510, que pasa la solicitud SIP BYE 566 a MGW 515. MGW 515 envía señales a MGW 520 con la solicitud ISUP REL 569. MGW 520 responde a MGW 515 con el mensaje 575 de ISUP RLC. MGW 515 responde al SBC 510 con el código de respuesta SIP 200 OK 572.

Entre el código de respuesta SIP 200 OK 560 y la solicitud SIP BYE 563, pueden ocurrir otros eventos. Específicamente, puede haber dos posibilidades alternativas 578: si la llamada es respondida por la parte llamada, el flujo de llamada incluye el flujo de llamada de la figura 7. Si la llamada no se establece correctamente, el flujo de llamadas incluye el flujo de llamadas de la figura 8.

La figura 7 es un diagrama que ilustra una parte de un flujo de llamadas según uno o más ejemplos. La figura 7 puede leerse junto con la figura 5 y como alternativa a la figura 8. Específicamente, la figura 7 representa la alternativa 777 en la que la llamada realizada en la figura 5 es contestada por la parte llamada. La figura 7 incluye MGW 715 y 720, SBC 710, SCP 725, centro de llamadas 705 y función de grabación de llamadas de plataforma de aplicación de red inteligente 790. Las MGW 715 y 720 pueden ser exactamente las MGW 515 y 520 como la figura 7 ilustra una alternativa 777 de una continuación de un flujo de llamadas que comienza en la figura 5. Los MGW 715 y 720 pueden ser el mismo equipo o un equipo similar y pueden realizarse en forma de Pasarela Serie Universal AS5400 de Cisco. Los MGW 715 y 720 pueden tener una conexión de parte de usuario ISDN (ISUP) contigua a través de un STP. El SBC 710 puede ser un MSC o SSP de terminación.

Un ISUP IAM 745 se envía desde MGW 715 a MGW 720 y puede ser exactamente ISUP IAM 545. Es decir, ISUP IAM 745 tiene como parámetros DRA1 y el número de la parte llamante. MGW 720 envía la solicitud SIP INVITE 742 al SBC 710 con un parámetro de DRA1. El SBC 710 envía una solicitud CAP 733 a SCP 725. Además, el mismo SCP/SCF está recibiendo la misma llamada, la primera vez que recibió la llamada se le indicó que la tratara con la lógica ServiceKey1, la próxima vez que el SCP / SCF sea contactado con esa llamada, debe ser con una solicitud para realizar una lógica diferente, por ejemplo, SK2 .... Donde 1 y 2 son arbitrarios pero predefinidos entre las SCF/SCP y las SSF/SSP.

Al recibir la solicitud CAP 733, SCP 725 toma la acción 736 de la siguiente manera. LaI D de correlación para la llamada se recupera de CdPBCDN. Se recuperan los detalles de la llamada introducidos en la ID de correlación. Una dirección de encaminamiento de destino se establece en el número de llamada original (OCN), es decir, el número del centro de llamadas. Se establece un número genérico (GN) con el calificador de número GN6 de manera que el parámetro número adicional de la parte llamante se establece en laID de correlación de la llamada. Los datos de detalles de llamadas adicionales se ingresan en laID de correlación y se almacenan. A continuación, SCP 725 envía mensajes 739 que comprenden un informe de solicitud BCSM (RRB) y CON al SBC 710. El mensaje RRB 739 puede incluir parámetros tales como fallo de selección de ruta, O_Called_Party_Busy, O_No_Answer, O_Answer, O_Disconnect u O_Abandon. El mensaje CON 739 puede incluir parámetros que establecen DRA en el número llamado original (OCN) y GN en la ID de correlación para la llamada.

El SBC 710 envía la solicitud SIP INVITE 730 al centro de llamadas 705. La solicitud SIP INVITE 730 incluye parámetros de OCN y GN, donde el GN se estableció en la ID de correlación para la llamada. El centro de llamadas 705 envía códigos de respuesta SIP (número de referencia 754) de 100, 188 o 183, según corresponda, al SBC 710, que transmite el código o códigos de respuesta 755 a MGW 720. MGW 720 envía el mensaje de dirección ISUP completa (ACM) 748 a MGW 715.

Continuando con el caso 777 donde se responde la llamada, el centro de llamadas 705 envía una respuesta SIP 200

OK 757 al SBC 710, que transmite el código de respuesta 758 al MGW 720. El MGW 720 responde al SBC 710 con la solicitud SIP ACK 778 y el SBC 710 transmite la solicitud 781 al centro de llamadas 705.

El SBC 710 envía el informe de eventos del punto de detección (DP) BCSM (ERB) O_Answer 784 a SCP 725. MGW 720 envía ISUP ANM 751 a MGW 715. ISUP ANM 751 puede ser exactamente ISUP ANM 551.

La función de grabación de llamadas de la plataforma de aplicaciones de red inteligente 790 clona y registra 787 la llamada.

Al recibir la solicitud SIP BYE 566, MGW 715 envía el mensaje ISUP REL 769 a MGW 720. El mensaje ISUP REL 769 puede ser exactamente ISUP REL 569. La MGW 720 envía la solicitud SIP BYE 766 al SBC 710, que envía DP O_Disconnect 793 a SCP 725. SCP 725 libera 796 la ID de correlación para la llamada para su posible reutilización. El SBC 710 también envía la solicitud SIP BYE 763 al centro de llamadas 705 que responde con la respuesta SIP 200 OK 760. El SBC 710 envía la respuesta SIP 200 OK 772 al MGW 720, y el MGW 720 envía el mensaje ISUP RLC 775 al MGW 715. El mensaje ISUP RLC 775 puede ser exactamente el mensaje 575 de ISUP RLC.

La figura 8 es un diagrama que ilustra una parte de un flujo de llamadas según una o más realizaciones de la presente invención. La figura 8 puede leerse junto con la figura 5 y como alternativa a la figura 7. Específicamente, la figura 8 representa la alternativa 888 en la que la llamada realizada en la figura 5 no se configuró correctamente. La figura 8 incluye las MGW 815 y 820, SBC 810, SCP 825 y el centro de llamadas 805. Las MGW 815 y 820 pueden ser exactamente las MGW 515 y 520 como en la figura 8 ilustra una alternativa 888 de una continuación de un flujo de llamadas que comienza en la figura 5. El SBC 810 puede ser un MSC o SSP de terminación.

Los ISUP IAM 845, solicitud SIP INVITE 842, solicitud CAP 833, acción 836, mensajes RRB y CON 839, solicitud SIP INVITE 830, códigos de respuesta SIP 854, códigos de respuesta SIP 855 y ISUP ACM 848 son exactamente ISUP IAM 745, solicitud SIP INVITE 742, solicitud CAP 733, acción 736, mensajes RRB y CON 739, solicitud SIP INVITE 730, códigos de respuesta SIP 754, códigos de respuesta SIP 755 e ISUP ACM 748, respectivamente, excepto que forman parte de la alternativa 888 donde hay una configuración de llamada incorrecta. En consecuencia, sus descripciones no se repetirán.

En el caso 888 donde hay una configuración de llamada fallida, el centro de llamadas 805 envía los códigos de respuesta SIP apropiados 857 de la serie 4xx y/o 5xx a SBC 810, que encamina los códigos de respuesta SIP 858 a MGW 820.

SBC 810 envía DP 893 O_DisconnectuO_Abandon a SCP 825, que luego libera 896 la ID de correlación asignada a la llamada para su posible reutilización.

MGW 820 envía el mensaje ISUP REL 869 a MGW 815, y MGW 815 responde a MGW 820 con el mensaje ISUP RLC 875. MGW 820 envía la solicitud SIP ACK 866 al SBC 810, que envía la solicitud SIP ACK 863 al centro de llamadas 805.

La figura 9 es un diagrama que ilustra un flujo de llamadas que incluye una función de bifurcación y una función de grabación de llamadas según uno o más ejemplos. La figura 9 incluye a la parte que llama 905, nodo (s) intermedio (s) 910 (si corresponde), MSC/SSP 915 del operador de terminación, plataforma de aplicación de red inteligente SCP 920, centro de llamadas 925, función de grabación de llamadas de plataforma de aplicación de red inteligente 930, hipertexto de plataforma de aplicación de red inteligente interfaz de programación de aplicaciones (API) de protocolo de transferencia (HTTP) frontal 935, función de grabación de llamadas de plataforma de aplicación de red inteligente 940, almacenamiento de datos de llamadas en memoria 945, bifurcación de tramo del operador de terminación/función 960 Acta de Refuerzo de la Leypara Asistencia de las Comunicaciones (CALEA), una sesión de ISUP o RTP de voz 970 desde la parte que llama 905 al centro de llamadas 925, un Servidor de Medios (MS) 985, una sesión de RTP de voz 980 que incluye una grabación de audio 959 grabada por MS 985 y un almacén de registro de datos de llamadas (CDR) 990 .

La figura 9 también incluye una pila que comprende multiplexión por división en el tiempo (TDM) 989, Protocolo de Internet (IP) con Protocolo de transmisión de Control deFlujo (SCTP) 991, Parte de Transferencia de Mensajes (MTP) Nivel 3 (MTP3) Capa de Adaptación de Usuario (M3UA) / Parte MTP Nivel 2 (MTP2) Capa de Adaptación de Usuario entre Pares (M2PA) 992, PU-RDSI 993, MTP 994, Parte de Control de Conexión de Señalización (SCCP) 995, Parte de Aplicación de Capacidades de Transacción (TCAP) 996, Parte de Aplicación Móvil (MAP) 997, Parte de Aplicación CAMEL (CAP) 998 y SCP 999, y capacidades e interfaces para el uso de los mismos, especialmente durante el registro de la llamada y la comparación de la ID de correlación de la llamada con los datos asociados con la ID de correlación de la llamada.

El teléfono 905 de la parte que llama envía la solicitud SIP INVITE 903 que se encamina al MSC o SSP 915 del operador de terminación (en adelante, "MSC/SSP 915").

En el caso de que el teléfono 905 de la parte que llama sea un teléfono móvil, MSC/SSP 915 envía una solicitud CAP 906 a SCP 920 con contexto de aplicación (AC) gsmssf a gsmscf y punto de detección inicial con parámetros relevantes. Los ejemplos de parámetros de IDP relevantes pueden incluir, entre otros, los siguientes: SK = 1033,

número de la parte llamante (CgPN), número de la parte llamada configurado en el número del centro de llamadas y EBCSM, incluidos parámetros como Información Recopilada, CallRefN y hora y zona horaria. SCP 920 responde a MSC/SSP 915 con el mensaje CAP CON 909. El mensaje CON 909 incluye los parámetros RRB, DRA establecido en ForkPrefix+CCNumber (número de centro de llamadas) y GN establecido en una ID de correlación para la llamada. El ForkPrefix está preconfigurado para forzar a MSC/SSP 915 a aplicar la bifurcación. El MSC/SSP 915 encamina 955 la llamada a una función de bifurcación debido al ForkPrefix en el mensaje DRA recibido 909 de CON.

El MSC/SSP 915 envía la solicitud SIP INVITE 912 a la función de bifurcación/CALEA 960 del tramo de la portadora de terminación (en adelante, "función de bifurcación 960"). La función de bifurcación 960 encamina 965 la llamada al centro de llamadas 925. Específicamente, la función de bifurcación 960 envía una solicitud 914 de ISUP IAM o SIP INVITE con parámetros que incluyen la ID de correlación de la llamada.

El centro de llamadas 925 intercambia información con la plataforma de aplicaciones de red inteligente HTTP API extremo 935 (en adelante, "extremo 935"). Este intercambio de información 918 incluye pasar la ID de correlación de la llamada desde el centro de llamadas 925 al extremo 935 y puede realizarse utilizando HTTP. El extremo 935 intercambia información (número de referencia 919), incluido la ID de correlación para la llamada, con la función de grabación de la plataforma de aplicación de red inteligente 930 (en adelante "función de grabación 930"). El extremo 935 también está en comunicación con un almacén de datos 945 y puede intercambiar información (número de referencia 924), incluido la ID de correlación de la llamada, con el almacén de datos 945. El almacén de datos 945 puede proporcionar, procesar y almacenar datos de llamadas en la memoria y/o en tiempo real.

El centro de llamadas 925 responde a la función de bifurcación 960 con el código de respuesta SIP 200 OK (número de referencia 927). La función de bifurcación 960 envía el código de respuesta SIP 200 OK (número de referencia 929) al MSC/SSP 915, que reenvía el código de respuesta 933 a la parte que llama. Se envía una solicitud SIP ACK 936 desde la parte llamante 905 al MSC/SSP 915, desde MSC/SSP 915 a la función de bifurcación 960 (número de referencia 939) y desde la función de bifurcación 960 al centro de llamadas 925 (número de referencia 942). MSC/SSP 915 envía el punto de detección ERB O_Answer 944 al SCP 920. Se inicia una sesión de ISUP o RTP de voz 970 desde la parte que llama 905 al centro de llamadas 925.

La función de bifurcación 960 bifurca 975 la sesión a la función de grabación 930. La función de bifurcación 960 envía una solicitud SIP INVITE 948 con parámetros que incluyen la ID de correlación para la llamada y SDP (Protocolo de descripción de SIP, que define la negociación entre dos partes que comparten medios). La función de grabación 930 envía una solicitud SIP INVITE 951 con el parámetro de SDP a la MS 985. La función de grabación 930 responde a la función de bifurcación 960 con el código de respuesta SIP 200 OK (número de referencia 954). La función de bifurcación 960 envía la solicitud SIP ACK 957 a la función de grabación 930. La sesión de RTP de voz 980 que incluye la llamada entre la parte que llama 905 y el centro de llamadas 925 comienza, y el audio se graba 959 por la MS 985.

Cuando la parte que llama 905 finaliza la llamada, se envía una solicitud SIP BYE 963 desde la parte que llama al MSC/SSP 915. El MSC/SSP 915 envía la solicitud SIP BYE 966 a la función de bifurcación 960, que a su vez envía el SIP Solicitud BYE 972 al centro de llamadas 925. El centro de llamadas 925 responde a la función de bifurcación 960 con el código de respuesta SIP 200 OK (número de referencia 973), y la función de bifurcación 960 envía el código de respuesta SIP 200 OK (número de referencia 974) al MSC/SSP 915. El MSC/SSP 915 envía el código de respuesta SIP 200 OK a la parte llamante 905 (número de referencia 978). El MSC/SSP 915 envía la solicitud SIP BYE 981 al centro de llamadas 925, que responde con el código de respuesta SIP 200 OK (número de referencia 984). El MSC/SSP 915 envía el mensaje RRB O_Disconnect 987 a SCP 920, y SCP 920 luego proporciona 988 un registro de detalles de llamada (CDR) relacionado con la llamada al almacén de datos 990. El CDR puede usarse con el propósito de una pista de auditoría, patrones de uso históricos, registros de facturación y métricas de rendimiento.

La figura 10 es un diagrama que ilustra un flujo de llamadas en el que la llamada no se encamina a una función de bifurcación según uno o más ejemplos. La figura 10 incluye la parte que llama 1005, nodo (s) intermedio (s) 1010 (si los hay), MSC/SSP 1015 del operador de terminación (en adelante "MSC/SSP 1015"), plataforma de aplicación de red inteligente SCP 1020, centro de llamadas 1025, llamada de plataforma de aplicación de red inteligente función de grabación 1030, función de bifurcación del tramo de la portadora de terminación/CALEA 1060 (de aquí en adelante "función de bifurcación 1060"), y una sesión RTP de voz 1070 desde la parte que llama 1005 al centro de llamadas 1025.

El teléfono 1005 de la parte que llama envía una solicitud SIP INVITE 1003 que finalmente llega al MSC/SSP 1015. En este momento, en el caso de que la llamada no se encamine a una función de bifurcación, existen al menos dos posibilidades 1013 alternativas que comprenden lo siguiente: alternativa 1023 en donde MSC/SSP 1015 tiene un diálogo de tiempo de espera o alternativa 1040 en donde MSC/SSP 1015 recibe una primitiva TCAP Abort 1011.

La alternativa 1023 comienza con la solicitud CAP 1006a y la alternativa 1040 comienza con la solicitud CAP 1006b. Las solicitudes CAP 1006a y 1006b son idénticas y se envían a SCP 1020. Las solicitudes CAP 1006a y 1006b pueden ser sustancialmente las mismas que las solicitudes CAP 906. En la alternativa 1023, se realiza un tiempo de espera de diálogo TCAP 1009. En la alternativa 1040, SCP 1020 responde a la solicitud CAP 1006b con la primitiva TCAP ABORT 1011.

MSC/SSP 1015 puede tener un disparador con manejo predeterminado configurado para continuar después de que ocurra una de las posibilidades en la alternativa 1013. Por consiguiente, la llamada no se encamina a la función de bifurcación 1060 y el establecimiento de la llamada continúa hacia el número CCNumber de la parte llamada original. (Número de referencia 1065.)

El MSC/SSP 1015 envía una solicitud SIP INVITE 1048 al centro de llamadas 1025, que responde al MSC/SSP 1015 con el código de respuesta SIP 200 OK (número de referencia 1054). El MSC/SSP 1015 envía el código de respuesta SIP 200 OK (número de referencia 1033) al teléfono 1005 de la persona que llama, que responde al MSC/SSP 1015 con la solicitud SIP ACK 1036. El MSC/SSP 1015 envía la solicitud SIP ACK 1057 al centro de llamadas 1025. Se inicia la sesión Voice RTP 1070 desde la persona que llama 1005 al centro de llamadas 1025. Al finalizar la llamada, el teléfono 1005 de la parte que llama envía una solicitud SIP BYE 1063 que llega al MSC/SSP 1015, y MSC/SSP 1015 envía una solicitud SIP BYE 1069 al centro de llamadas 1025. El centro de llamadas 1025 envía el código de respuesta SIP 200 OK (número de referencia 1072) al MSC/SSP 1015, que reenvía el código de respuesta SIP 200 OK (número de referencia 1078) al teléfono 1005 de la persona que llama.

La plataforma de aplicación de red inteligente 250, las instalaciones de red de próxima generación seguras 320, la plataforma de aplicación de red inteligente 435 pueden realizarse además con uno o más procesadores y un dispositivo de memoria. La figura 6 es un ejemplo más detallado de tales detalles de ejecución de hardware.

La figura 6 es un diagrama de bloques de alto nivel de un ordenador de ejemplo (600) que está dispuesto para identificar amenazas a través del análisis de señales de comunicaciones, eventos y/o participantes. El ordenador (600) puede usarse para realizar adicionalmente la plataforma de aplicación de red inteligente 250, las instalaciones de red de próxima generación 320 seguras y la plataforma de aplicación de red inteligente 435, realizaciones de la invención que pueden ser denominadas colectiva e individualmente en el presente documento como una "plataforma de aplicación de red". o "plataforma de aplicaciones de redes de telecomunicaciones".

En una configuración muy básica (601), el dispositivo de ordenador (600) incluye típicamente uno o más procesadores (610) y memoria del sistema (620). Se puede usar un bus del sistema (630) para comunicarse entre el procesador (610) y la memoria del sistema (620).

Dependiendo de la configuración deseada, el procesador (610) puede ser de cualquier tipo, incluidos, entre otros, un microprocesador (µP), un microcontrolador (µC), un procesador digital de señales (DSP) o cualquier combinación de los mismos. El procesador (610) puede incluir un nivel más de almacenamiento en memoria intermedia, un núcleo de procesador y registros. El núcleo del procesador puede incluir una unidad lógica aritmética (ALU), una unidad de punto flotante (FPU), un núcleo de procesamiento de señales digitales (DSP Core) o cualquier combinación de los mismos. También se puede utilizar un controlador de memoria con el procesador (610) o, en algunas ejecuciones, el controlador de memoria puede ser una parte interna del procesador (610).

Dependiendo de la configuración deseada, la memoria del sistema (620) puede ser de cualquier tipo que incluye, pero no se limita a, memoria volátil (como RAM), memoria no volátil (como ROM, memoria flash, etc.) o cualquier combinación de las mismas. La memoria del sistema (620) incluye típicamente un sistema operativo (621), una o más aplicaciones (622) y datos de programa (624). La aplicación (622) puede incluir un sistema y método para identificar amenazas a través del análisis de señales de comunicaciones, eventos y/o participantes como se describe anteriormente en relación con las figuras 3, 4, 5, 7, 8, 9, 10 y 11a-c. Los datos del programa (624) incluyen el almacenamiento de instrucciones que, cuando son ejecutadas por uno o más dispositivos de procesamiento, realizan un sistema y método para identificar amenazas a través del análisis de señales de comunicaciones, eventos y/o participantes (623). En algunas realizaciones, la aplicación (622) puede disponerse para operar con datos de programa (624) en un sistema operativo (621). Los datos de programa (624) incluyen datos de servicio (625). Los datos de servicio (625) representan datos particulares de la instancia que se va a procesar, por ejemplo, variables no inicializadas, que pueden incluir argumentos para parámetros de métodos apropiados para realizar los sistemas y métodos descritos en este documento.

El dispositivo de ordenador (600) puede tener características o funciones adicionales e interfaces adicionales para facilitar las comunicaciones entre la configuración básica (601) y cualquier dispositivo e interfaz necesarios, como el interfaz de memoria no volátil no extraíble (670), el interfaz de memoria no volátil extraíble interfaz (660), el interfaz de entrada de usuario (650), el interfaz de red (640) y el interfaz periférico de salida (635). Se puede conectar una unidad de disco duro o una unidad de estado sólido (SSD) al bus del sistema (630) a través de un interfaz de memoria no volátil no extraíble (670). Se puede conectar una unidad de disco magnético u óptico al bus del sistema (630) mediante el interfaz no volátil extraíble (660). Un usuario del dispositivo de ordenador (600) puede interactuar con el dispositivo de ordenador (600) a través de dispositivos de entrada tales como teclado, ratón u otro periférico de entrada conectado a través de un interfaz de entrada de usuario (650). Se puede conectar un monitor, impresora, altavoz u otro dispositivo periférico de salida al dispositivo informático (600) a través de un interfaz periférico de salida (635) para proporcionar salida desde el dispositivo de ordenador (600) a un usuario u otro dispositivo.

La memoria del sistema (620) es un ejemplo de medio de almacenamiento de ordenador. Los medios de almacenamiento de ordenador incluyen, pero no se limitan a, RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) u otro almacenamiento óptico, casetes magnéticos, cinta

magnética, almacenamiento en disco magnético u otro dispositivos de almacenamiento magnético, o cualquier otro medio que se pueda utilizar para almacenar la información deseada y al que se pueda acceder mediante el dispositivo de ordenador (600). Cualquiera de estos medios de almacenamiento de ordenador puede formar parte del dispositivo (400). Se pueden conectar una o más unidades de procesamiento de gráficos (GPU) (699) al bus del sistema (630) para proporcionar capacidad de cálculo en coordinación con el procesador (610), especialmente donde están presentes problemas de instrucción única, datos múltiples (SIMD).

El dispositivo de ordenador (600) se puede realizar como una parte de un dispositivo electrónico portátil (o móvil) de factor de forma pequeño, como un teléfono celular, un teléfono inteligente, un asistente de datos personales (PDA), un dispositivo reproductor multimedia personal, un tableta (tableta), un dispositivo de vigilancia de web inalámbrico, un dispositivo de auricular personal, un dispositivo de aplicación específica o un dispositivo híbrido que incluya cualquiera de las funciones anteriores. El dispositivo de ordenador (600) también se puede realizar como un ordenador personal que incluye configuraciones de ordenador portátil y de ordenador no portátil. Además, el dispositivo de ordenador (600) puede funcionar en un entorno de red en el que está conectado a uno o más ordenadores remotos a través de una red utilizando el interfaz de red (650).

La figura 11a es un diagrama de bloques que ilustra un método para la identificación de amenazas a través del análisis de señales de comunicaciones, eventos y/o participantes de acuerdo con uno o más ejemplos. Los métodos de las figuras 11a se realizan por y desde la perspectiva de cualquiera de la plataforma de aplicación de red inteligente 250, las instalaciones de red de próxima generación segura 320 o la plataforma de aplicación de red inteligente 435 que pueden denominarse colectivamente en el presente documento como "plataforma de aplicación de red inteligente".

Primero, una plataforma de aplicación de red inteligente recibe una señal (por ejemplo, una solicitud SS7 o una solicitud MAP o una solicitud CAP o una solicitud API) de las instalaciones de señalización del operador en el lado de origen de la llamada (1210). La plataforma de aplicaciones de red inteligente luego almacena los datos del borde exterior de la persona que llama (1220). A continuación, la plataforma de aplicaciones de red inteligente analiza los datos del borde exterior de origen (desde las instalaciones del operador en el lado de origen de la llamada) con los datos del borde exterior históricos o en tiempo real para determinar un puntaje de amenaza (1260). Se observa que el "puntaje de amenaza" puede ser un solo número que indica un grado de amenaza potencial que representa la llamada pero, en la práctica, la puntuación de amenaza abarca un conjunto de parámetros. Este conjunto de parámetros puede incluir resultados negativos, positivos o neutrales de cada uno de los puntos de análisis, como coincidencia de red, coincidencia de proximidad, hora del día, actividad social, autenticación de múltiples factores y otros elementos similares disponibles ahora y en el futuro para corroborar a los participantes en la convocatoria.

Además, los métodos para determinar el puntaje de amenaza (1260, 1262, 1264 y 1266 en las figuras 11a-d), en sí mismos, son procesos convencionales conocidos y todos los cálculos de puntaje de amenaza conocidos y desarrollados en el futuro están dentro del alcance de las varias invenciones descritas en este documento. Ejemplos no limitativos de tales procesos de cálculo de puntaje de amenaza convencionales incluyen determinar la ruta que tomó la llamada para llegar al punto supervisado en la configuración de la llamada a través de códigos de punto, comparando el tipo de línea de origen con el tipo de número de teléfono, comparando la identidad del p-afirmado del usuario que proporcionó el número de teléfono de la parte que llama, comparar la ubicación del origen de la llamada con la ubicación actual del número de teléfono, comparar el número de teléfono de la parte que llama con listas públicas y privadas y sistemas de quejas, telemarketing/robots de llamadas conocidos, estados de llamadas conocidos y números conocidos falsos/no asignados. Los aspectos de la presente descripción mejoran en gran medida dichos cálculos de puntaje de amenaza al aprovechar la señalización de llamadas que proporciona una colección más rica y de datos más fiables para su uso en dichos cálculos de puntaje de amenaza.

A partir de entonces, la plataforma de aplicación de red inteligente puede tomar una o más acciones (1290) tales como proporcionar datos de puntaje en tiempo real con respecto a la llamada a la parte llamada, enviar una señal al operador para terminar la llamada, enviar una señal al operador para encaminar la llamada a las fuerzas del orden público o notifique a las fuerzas del orden público sobre la llamada de alto puntaje de amenaza, y/o informe a los propietarios de la red sobre las instalaciones de la red potencialmente comprometidas. Las acciones también pueden incluir acciones dinámicas o predeterminadas tales como redirigir la llamada telefónica a un nuevo destino, tal como un agente altamente calificado, un sistema IVR/VRU para autenticación automatizada o correo de voz; dividir el audio en una instalación de grabación, supervisión o escucha; y/o colgar a la persona que llama.

La figura 11b ilustra, por ejemplo, un caso en el que el teléfono 310 ha realizado una llamada a las instalaciones 315 del operador y la llamada ha sido recibida por un centro de llamadas de clientes empresariales 355 u otro nodo (terminal o intermedio). Además de los pasos 1210, 1220, 1290 que se describen anteriormente, se pueden realizar los siguientes pasos adicionales. Un paso opcional es que la plataforma de aplicación de red inteligente envíe un mensaje de reanudación a las instalaciones de señalización del operador en el lado de origen de la llamada (1230). La plataforma de aplicación de red inteligente también recibe una señal (por ejemplo, solicitud SS7 o solicitud MAP o solicitud CAP o solicitud API) de las instalaciones de señalización del operador en el lado de terminación de la llamada (1240). La plataforma de aplicación de red inteligente puede enviar opcionalmente una instrucción para unirse a la llamada y/o supervisión de eventos a las instalaciones de señalización del operador en el lado de terminación de la llamada (1250). A continuación, la plataforma de aplicación de red inteligente compara o analiza de otro modo los datos del borde exterior que se originan (de las instalaciones del operador en el lado de origen de la llamada) con los

datos del borde del exterior del lado de la terminación (1262) para determinar una puntaje de amenaza (1262). Debido a la vulnerabilidad de los datos dentro de la red de comunicaciones, dichos datos del borde exterior pueden modificarse o verse comprometidos de alguna manera. Por lo tanto, al analizar los datos del borde exterior del lado de origen antes de que las entidades maliciosas puedan cambiar los datos del borde exterior contra los datos del borde exterior del lado de terminación, se pueden detectar tales cambios o compromisos de datos. Se observa además que esta comparación/análisis (1262) puede realizarse utilizando datos de borde exterior de un nodo intermedio (por ejemplo, instalaciones de la portadora 335 en la figura 3) y/o nodo de terminación (por ejemplo, galope de llamada de cliente empresarial 355). 11c ilustra, por ejemplo, un caso en el que el teléfono 310 ha realizado una llamada a las instalaciones 315 del operador y la llamada ha sido recibida por un centro de llamadas de clientes empresariales 355 u otro nodo (terminal o intermedio). Además de los pasos 1210, 1220, 1230, 1290 que se describen anteriormente, se pueden realizar los siguientes pasos adicionales.

La figura 11c agrega captura, almacenamiento y análisis de datos del borde interno. Los datos del borde interior se pueden recopilar de nodos intermedios. Los datos del borde interior pueden incluir nuevos datos en combinación o como reemplazo de los datos del borde exterior, así como cualquier nodo intermedio que participó entre el borde exterior y el borde interior supervisado. El borde exterior acompañante o los datos del nodo participante previo pueden ser la información exacta, abstraída/traducida o diferente que los datos respectivos disponibles en el borde exterior y los datos del nodo anterior. Por ejemplo, la ID de célula desde la cual una llamada telefónica originada en un móvil puede estar disponible como el identificador (número) en bruto en los datos del borde exterior, pero los datos respectivos en los datos del borde interior pueden haber sido transformados por un nodo intermedio para ser el código postal de donde reside ese ID de celda o está más cerca. De manera similar, los nodos intermedios pueden inyectar sus propios datos o decisiones de encaminamiento, como el desvío de llamadas, que da como resultado que los datos de la parte llamada original de los datos del borde exterior se incluyan en un nuevo campo (por ejemplo, número de parte llamada original) y el valor modificado del nodo intermedio para el número de la parte llamada es el número reenviado. Se espera que esta variación sea posible y útil cuando ocurre y no ocurre porque los aspectos de la invención pueden usar las inconsistencias estadísticas relativas para ayudar a identificar posibles participantes inesperados en una llamada futura. La figura 11c añade un paso de recepción 1240 que recibe, en la plataforma de aplicación de red inteligente, una señal (por ejemplo, solicitud SS7 o solicitud MAP o solicitud CAP o solicitud API) de las instalaciones de señalización de la portadora de un nodo intermedio. En respuesta, los datos del borde interior se almacenan (1245). Se observa que pueden usarse múltiples solicitudes a múltiples nodos intermedios diferentes (por ejemplo, un bucle de los pasos 1240 y 1245) para capturar y almacenar datos del borde interno de múltiples nodos intermedios. A continuación, la plataforma de aplicación de red inteligente compara o analiza de otro modo los datos del borde externo (de las instalaciones del operador en el lado de origen de la llamada y/o en el lado de terminación de la llamada) con los datos del borde interno (de uno o más nodos intermedios) para determinar una puntaje de amenaza (1264).

La figura 11d aprovecha la captura, el almacenamiento y el análisis de datos del borde interno en múltiples nodos intermedios. Primero, una plataforma de aplicación de red inteligente recibe una señal (por ejemplo, una solicitud SS7 o solicitud MAP o solicitud CAP o solicitud API) de las instalaciones de señalización de la portadora de un primer nodo intermedio (1215). La plataforma de aplicaciones de red inteligente luego almacena los datos del borde interno de la llamada (1220) de ese primer nodo intermedio. La plataforma de aplicación de red inteligente puede recibir entonces otra señal (por ejemplo, una solicitud SS7 o una solicitud MAP o una solicitud CAP o una solicitud API) de las instalaciones de señalización de la portadora de un segundo nodo intermedio (1242). La plataforma de aplicaciones de red inteligente luego almacena los datos del borde interno de la llamada (1245) de ese segundo nodo intermedio. Se observa que un aspecto de la invención puede llevar a cabo una captura y almacenamiento adicionales de datos del borde interno de otros ($3^{ésimo}$, $4^{ésimo}$, ... ésimo) nodos intermedios. La plataforma de aplicación de red inteligente puede comparar o analizar de otro modo los datos del borde interno del primer nodo intermedio con los datos del borde interno (de uno o más de otros nodos intermedios) para determinar una puntaje de amenaza (1266).

La figura 12 es un diagrama de bloques que ilustra un método para etiquetar una llamada con un identificador de correlación tanto en el extremo de origen como en el de terminación de la llamada de acuerdo con uno o más ejemplos. Primero, el teléfono de la parte que llama envía una solicitud SIP INVITE al SSP o MSC en el lado de origen de la llamada (1310). En segundo lugar, un SCP que forma parte de la plataforma de aplicaciones de red inteligente recibe una solicitud de CAP con parámetros relevantes del SSP o MSC en el lado de origen de la llamada (1320). En tercer lugar, la plataforma de aplicaciones de red inteligente crea una ID de correlación para la llamada (1330). En cuarto lugar, un SCP que forma parte de la plataforma de aplicación de red inteligente envía una solicitud de CAP con los parámetros relevantes, incluido la ID de correlación de la llamada, al SSP o MSC en el lado de terminación de la llamada (1340). En quinto lugar, un centro de llamadas recibe una solicitud SIP INVITE con parámetros relevantes, incluido la ID de correlación para la llamada, del SSP o MSC en el lado de terminación de la llamada (1350).

La descripción detallada anterior ha establecido varios ejemplos de los dispositivos y/o procesos mediante el uso de diagramas de bloques, diagramas de flujo y/o ejemplos. En la medida en que dichos diagramas de bloques, diagramas de flujo y/o ejemplos contengan una o más funciones y/u operaciones, aquellos dentro de la técnica entenderán que cada función y/u operación dentro de dichos diagramas de bloques, diagramas de flujo o ejemplos se puede realizar, individual y/o colectivamente, mediante una amplia gama de hardware, software, firmware o prácticamente cualquier combinación de los mismos. Los expertos en la técnica apreciarán que los mecanismos del tema descrito en el presente documento pueden distribuirse como un producto de programa en una variedad de formas, y que un ejemplo

ilustrativo del tema descrito en este documento se aplica independientemente del tipo particular de medio portador de señales no transitorias utilizado para llevar a cabo la distribución. Los ejemplos de un medio portador de señales no transitorias incluyen, entre otros, los siguientes: un medio de tipo grabable, como un disquete, una unidad de disco duro, un disco compacto (CD), un disco de vídeo digital (DVD), una cinta digital, una memoria de computadora, etc.; y un medio del tipo de transmisión tal como un medio de comunicación digital y/o analógico. (por ejemplo, un cable de fibra óptica, una guía de ondas, un enlace de comunicaciones por cable, un enlace de comunicaciones inalámbricas, etc.)

Con respecto al uso de sustancialmente cualquier término en plural y/o singular en este documento, los expertos en la técnica pueden traducir del plural al singular y/o del singular al plural según sea apropiado para el contexto y/o aplicación. Las diversas permutaciones de singular/plural se pueden establecer expresamente en este documento por motivos de claridad.

Por tanto, se han descrito ejemplos particulares del tema. Otros ejemplos están dentro del alcance de las siguientes reivindicaciones. Además, los procesos representados en las figuras adjuntas no requieren necesariamente el orden particular mostrado, o el orden secuencial, para lograr resultados deseables. En ciertas ejecuciones, la multitarea y el procesamiento en paralelo pueden resultar ventajosos.

REIVINDICACIONES

1. Un método para determinar una puntuación de amenaza de una llamada que atraviesa una red de telecomunicaciones, que comprende:

recibir (1210), mediante una plataforma de aplicación de red, datos del borde exterior de una primera señal desde instalaciones de señalización de la portadora de origen en un lado de origen de la llamada;

recibir (1240), mediante la plataforma de aplicación de red, datos del borde de terminación de una segunda señal desde un nodo de red de telecomunicaciones en un lado de terminación de la llamada;

analizar (1262), mediante la plataforma de aplicación de red, los datos del borde exterior frente a los datos del borde de terminación para determinar una puntuación de amenaza que represente un grado de amenaza de la llamada; y

redirigir (1290), mediante la plataforma de aplicaciones de red, la llamada a un nuevo destino en respuesta a la puntuación de amenaza.

2. El método de la reivindicación 1, que además comprende:

tomar (1290) una acción en respuesta a la puntuación de amenaza en la que la acción incluye uno o más de proporcionar la puntuación de amenaza a la parte llamada; informar al propietario de la red o al proxy del mismo sobre una red potencialmente comprometida; redirigir la llamada a un agente altamente capacitado, un sistema IVR/VRU para la autenticación automatizada o correo de voz; dividir el audio de la llamada a una instalación de grabación, supervisión o escucha; o colgar a la persona que llama.

3. El método de la reivindicación 1, que además comprende:

analizar (1262) los datos del borde exterior con los datos del borde de terminación, cualquier dato de nodo intermedio disponible, datos históricos y datos en tiempo real para determinar la puntuación de amenaza.

4. El método de la reivindicación 1, que además comprende:

recibir (1240), en la plataforma de aplicación de red, una señal de un nodo de red de telecomunicaciones intermedio (910, 1010,335,1215,1242);

almacenar (1245) datos de borde interno relacionados con la llamada que ha atravesado al menos parcialmente la red de telecomunicaciones hasta el nodo intermedio (910, 1010, 335, 1215, 1242); y

analizar (1264) los datos del borde exterior frente a los datos del borde interior, los datos históricos y los datos en tiempo real para determinar el puntaje de amenaza.

5. El método de la reivindicación 1, en el que la señal de las instalaciones de señalización de la portadora de origen en un lado de origen de la llamada es una o más de una solicitud SS7, solicitud MAP, solicitud CAP o API.

6. Un método para determinar un puntaje de amenaza de una llamada que atraviesa una red de telecomunicaciones, que comprende:

recibir (1215), mediante una plataforma de aplicación de red, datos del primer borde interno de una señal de las instalaciones de señalización de la portadora en un primer nodo intermedio (1215) de la red de telecomunicaciones;

recibir (1242), mediante la plataforma de aplicación de red, datos del segundo borde interno de otra señal de las instalaciones de señalización de la portadora en un segundo nodo intermedio (1242) de la red de telecomunicaciones;

analizar (1266), mediante la plataforma de aplicaciones de red, los datos del primer borde interno frente a los datos del segundo borde interno para determinar un puntaje de amenaza que representa un grado de amenaza de la llamada; y

redirigir (1290), por la plataforma de aplicaciones de red, la llamada a un nuevo destino en respuesta al puntaje de amenaza.

7. El método de la reivindicación 6, que comprende además:

tomar (1290) una acción en respuesta al puntaje de amenaza en la que la acción incluye uno o más de proporcionar el puntaje de amenaza a la parte llamada; informar al propietario de la red o al proxy del mismo sobre una red potencialmente comprometida; redirigir la llamada a un agente altamente capacitado, un sistema IVR/VRU para la autenticación automatizada o correo de voz; dividir el audio de la llamada a una instalación de grabación, supervisión o escucha; o colgar a la persona que llama.

8. El método de la reivindicación 6, en el que las señales de las instalaciones de señalización de la portadora en un lado de origen de la llamada son una o más de una solicitud SS7, solicitud MAP, solicitud CAP o API.

9. Una plataforma de aplicaciones de redes de telecomunicaciones (290, 320, 450), que comprende:

un procesador (610);

un dispositivo de memoria (620) que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el procesador:

reciba (1210), en la plataforma de aplicación de la red de telecomunicaciones, datos del borde exterior de una primera señal de las instalaciones de señalización de la portadora de origen en un lado de origen de la llamada;

reciba (1240), en la plataforma de aplicación de la red de telecomunicaciones, datos del borde de terminación de una segunda señal desde un nodo de red de telecomunicaciones en un lado de terminación de la llamada;

analice (1260), en la plataforma de aplicación de la red de telecomunicaciones, los datos del borde exterior frente a los datos del borde de terminación para determinar un puntaje de amenaza que represente un grado de amenaza de la llamada; y

redirija (1290) la llamada a un nuevo destino en respuesta al puntaje de amenaza.

10. La plataforma de aplicaciones de red de telecomunicaciones de la reivindicación 9, en la que el dispositivo de memoria almacena instrucciones adicionales que, cuando son ejecutadas por el procesador, hacen que el procesador:

tome (1290) una acción en respuesta al puntaje de amenaza en la que la acción incluye una o más de proporcionar el puntaje de amenaza a la parte llamada; informar al propietario de la red o al proxy del mismo sobre una red potencialmente comprometida; redirigir la llamada a un agente altamente capacitado, un sistema IVR/VRU para autenticación automatizada o correo de voz; dividir el audio de la llamada a una instalación de grabación, supervisión o escucha; o colgar a la persona que llama.

11. La plataforma de aplicaciones de red de telecomunicaciones de la reivindicación 9, en la que el dispositivo de memoria almacena instrucciones adicionales que, cuando son ejecutadas por el procesador, hacen que el procesador:

almacene los datos del borde exterior actualizados relacionados con la llamada que ha atravesado al menos parcialmente la red de telecomunicaciones; y

analice (1262) los datos del borde exterior frente a los datos del borde exterior actualizados para determinar el puntaje de amenaza.

12. La plataforma de aplicaciones de red de telecomunicaciones de la reivindicación 9, en la que el dispositivo de memoria almacena instrucciones adicionales que, cuando son ejecutadas por el procesador, hacen que el procesador:

reciba (1240), en la plataforma de aplicación de red, una señal de un nodo de red de telecomunicaciones intermedio (910, 1010, 335, 1215, 1242);

almacene los datos de borde interno relacionados con la llamada que ha atravesado al menos parcialmente la red de telecomunicaciones hasta el nodo intermedio (910, 1010, 335, 1215, 1242); y

analice (1264) los datos del borde exterior frente a los datos del borde interior para determinar el puntaje de amenaza.

13. Una plataforma de aplicaciones de redes de telecomunicaciones (220, 320, 450), que comprende:

un procesador (610);

un dispositivo de memoria (620) que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el procesador:

reciba (1215), mediante una plataforma de aplicación de red, los primeros datos del borde interno en una primera señal de las instalaciones de señalización de la portadora en un primer nodo intermedio (1215) de la red de telecomunicaciones;

reciba (1242), mediante la plataforma de aplicación de red, datos del segundo borde interno de otra señal de las instalaciones de señalización de la portadora en un segundo nodo intermedio (1242) de la red de telecomunicaciones;

analice (1266), mediante la plataforma de aplicaciones de red, los datos del primer borde interno frente a los datos del segundo borde interno para determinar un puntaje de amenaza que represente un grado de amenaza de una llamada; y

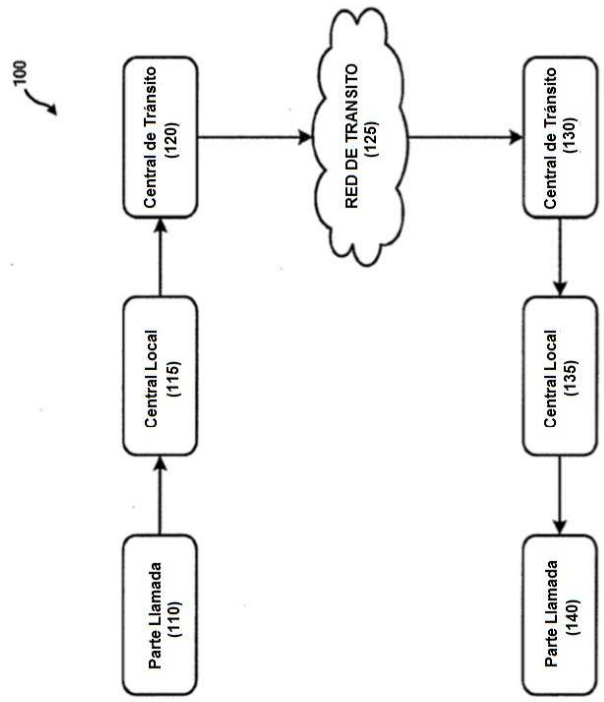
redirija, mediante la plataforma de aplicaciones de red, la llamada a un nuevo destino en respuesta al puntaje de amenaza.

14. La plataforma de aplicaciones de red de telecomunicaciones de la reivindicación 13, en la que el dispositivo de

memoria almacena instrucciones adicionales que, cuando son ejecutadas por el procesador, hacen que el procesador:

tome (1290) una acción en respuesta al puntaje de amenaza en la que la acción incluye una o más de proporcionar el puntaje de amenaza a la parte llamada; informar al propietario de la red o al proxy del mismo sobre una red potencialmente comprometida; redirigir la llamada a un agente altamente capacitado, un sistema IVR/VRU para autenticación automatizada o correo de voz; dividir el audio de la llamada a una instalación de grabación, supervisión o escucha; o colgar a la persona que llama.

15. La plataforma de aplicación de red de telecomunicaciones de la reivindicación 9 o la reivindicación 14, en la que las señales de las instalaciones de señalización de la portadora en un lado de origen de la llamada son una o más de una solicitud SS7, solicitud MAP, solicitud CAP o API.



Técnica Convencional

FIG. 1

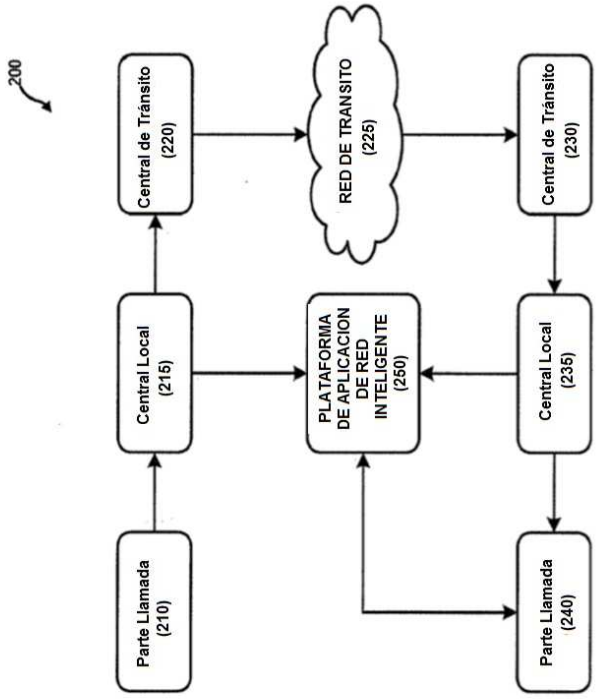

200
Central de Tránsito (220)
RED DE TRANSITO (225)
Central de Tránsito (230)
Central Local (215)
PLATAFORMA DE APLICACION DE RED INTELIGENTE (250)
Central Local (235)
Parte Llamada (210)
Parte Llamada (240)

FIG. 2

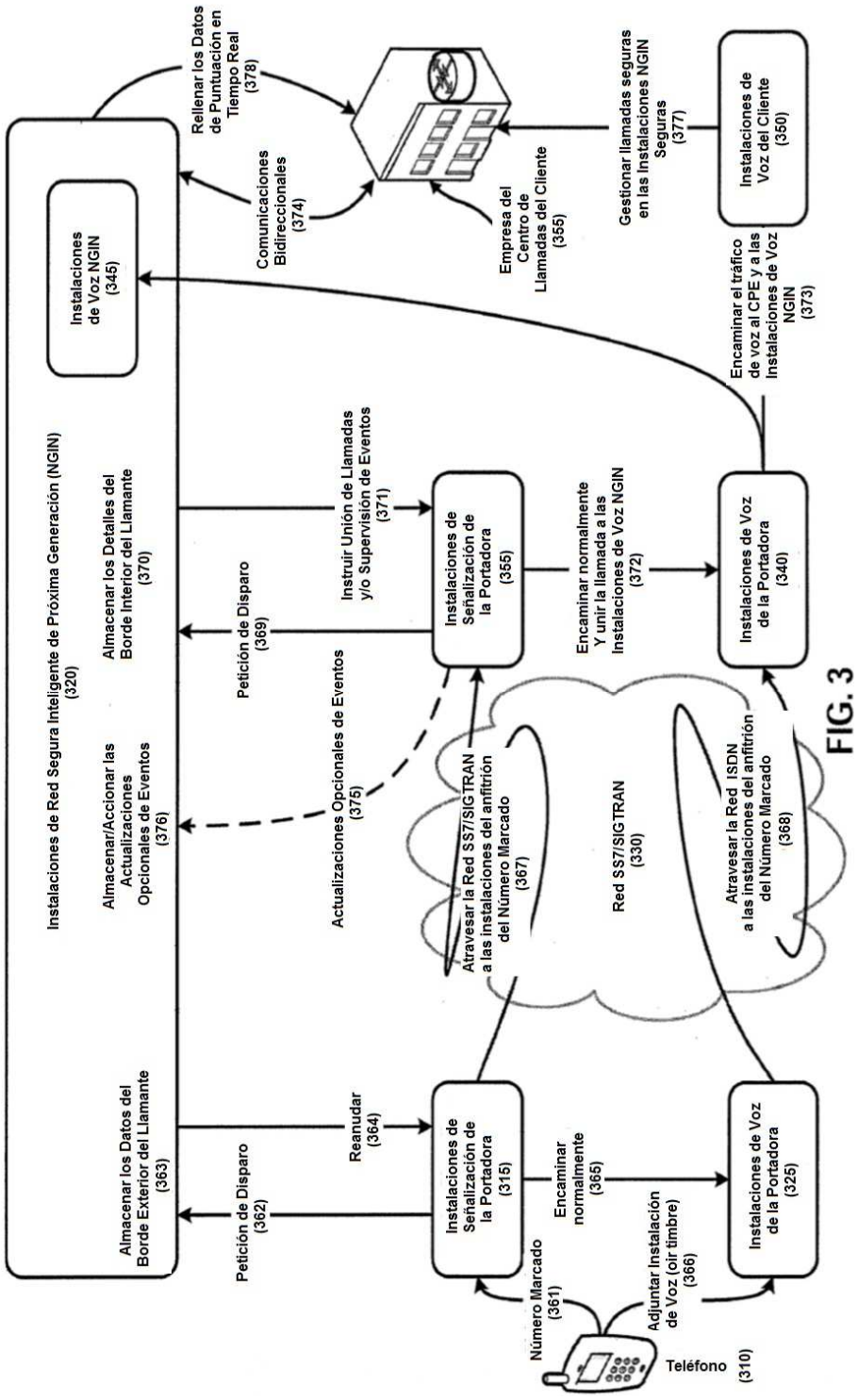

Instalaciones de Red Segura Inteligente de Próxima Generación (NGIN) (320)
Instalaciones de Voz NGIN (345)
Rellenar los Datos de Puntuación en Tiempo Real (378)
Comunicaciones Bidireccionales (374)
Empresa del Centro de Llamadas del Cliente (355)
Gestionar llamadas seguras en las Instalaciones NGIN Seguras (377)
Instalaciones de Voz del Cliente (350)
Encaminar el tráfico de voz al CPE y a las Instalaciones de Voz NGIN (373)
Almacenar los Datos del Borde Exterior del Llamante (363)
Almacenar los Detalles del Borde Interior del Llamante (370)
Almacenar/Accionar las Actualizaciones Opcionales de Eventos (376)
Petición de Disparo (362)
Petición de Disparo (369)
Reanudar (364)
Instruir Unión de Llamadas y/o Supervisión de Eventos (371)
Actualizaciones Opcionales de Eventos (375)
Instalaciones de Señalización de la Portadora (315)
Instalaciones de Señalización de la Portadora (355)
Encaminar normalmente (365)
Encaminar normalmente Y unir la llamada a las Instalaciones de Voz NGIN (372)
Instalaciones de Voz de la Portadora (325)
Instalaciones de Voz de la Portadora (340)
Atravesar la Red SS7/SIGTRAN a las instalaciones del anfitrión del Número Marcado (367)
Red SS7/SIGTRAN (330)
Atravesar la Red ISDN a las instalaciones del anfitrión del Número Marcado (368)
Número Marcado (361)
Adjuntar Instalación de Voz (oír timbre) (366)
Teléfono (310)

FIG. 3

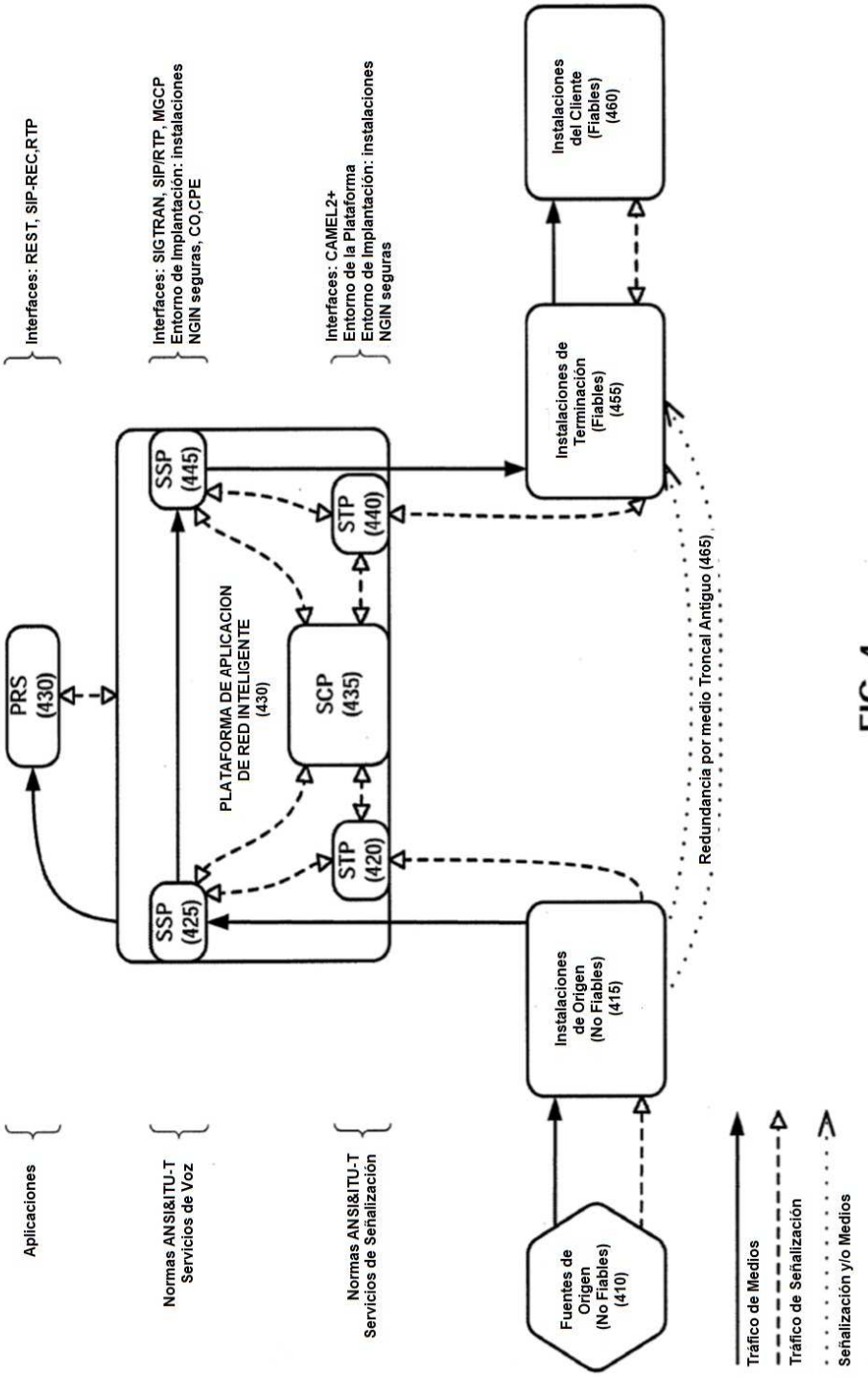

Interfaces: REST, SIP-REC,RTP
Interfaces: SIGTRAN, SIP/RTP, MGCP
Entorno de Implantación: instalaciones
NGIN seguras, CO,CPE
Interfaces: CAMEL2+
Entorno de la Plataforma
Entorno de implantación: instalaciones
NGIN seguras
Instalaciones del Cliente (Fiables) (460)
Instalaciones de Terminación (Fiables) (455)
SSP (445)
STP (440)
PRS (430)
PLATAFORMA DE APLICACION DE RED INTELIGENTE (430)
SCP (435)
STP (420)
SSP (425)
Redundancia por medio Troncal Antiguo (465)
Instalaciones de Origen (No Fiables) (415)
Fuentes de Origen (No Fiables) (410)
Aplicaciones
Normas ANSI&ITU-T Servicios de Voz
Normas ANSI&ITU-T Servicios de Señalización
Tráfico de Medios
Tráfico de Señalización
Señalización y/o Medios

FIG. 4

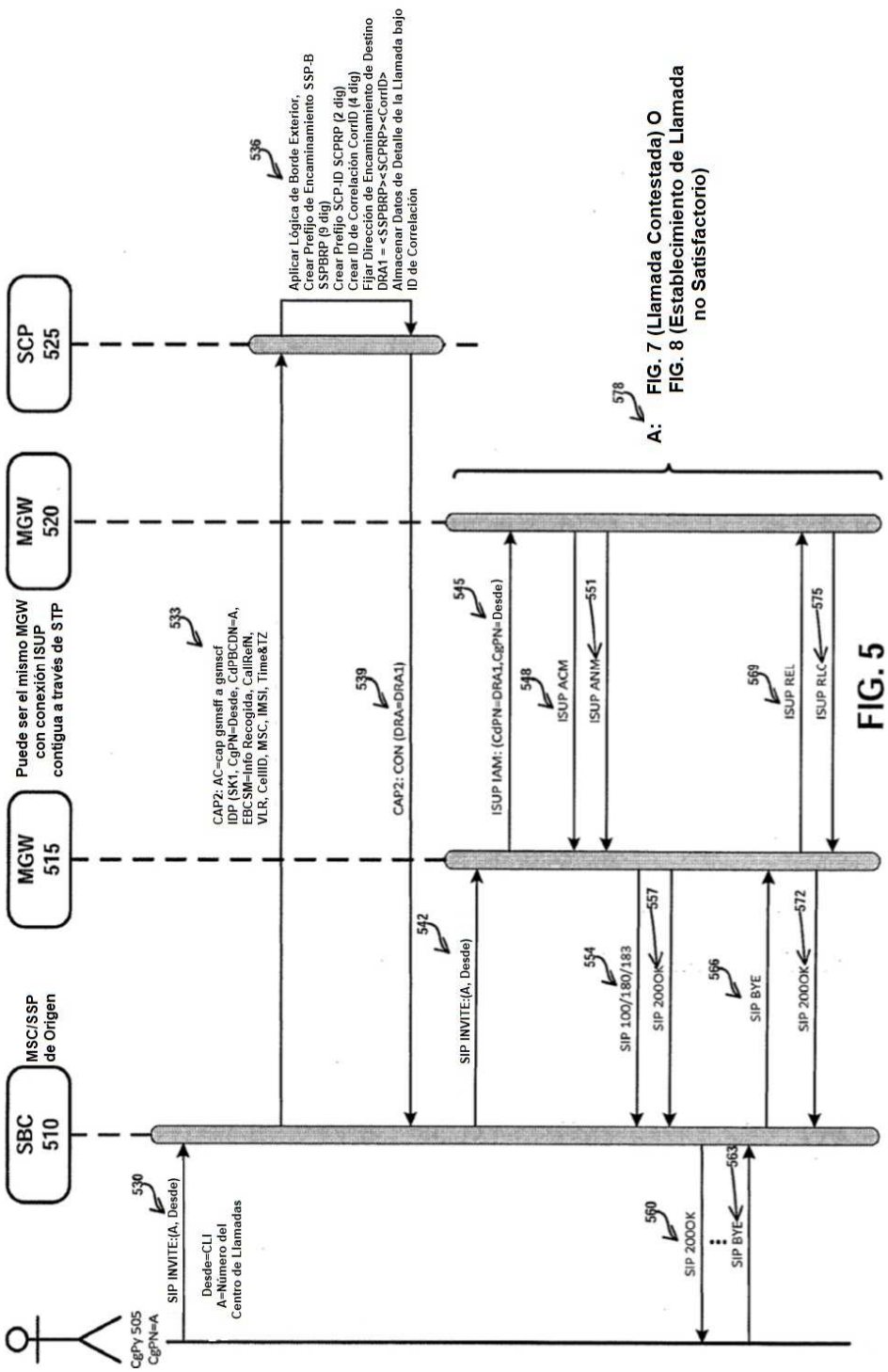

SBC 510
MSC/SSP de Origen
MGW 515
Puede ser el mismo MGW con conexión ISUP contigua a través de STP
MGW 520
SCP 525
CgPy 505
CgPN=A
SIP INVITE:(A, Desde)
530
Desde=CLI
A=Número del Centro de Llamadas
Aplicar Lógica de Borde Exterior, Crear Prefijo de Encaminamiento SSP-B SSPBRP (9 dig) Crear Prefijo SCP-ID SCPRP (2 dig) Crear ID de Correlación CorrID (4 dig) Fijar Dirección de Encaminamiento de Destino DRA1 = <SSPBRP><SCPRP><CorrID> Almacenar Datos de Detalle de la Llamada bajo ID de Correlación
536
CAP2: AC=cap gsmsff a gsmscf IDP (SK1, CgPN=Desde, CdPBCDN=A, EBCSM=Info Recogida, CallRefN, VLR, CellID, MSC, IMSI, Time&TZ
533
CAP2: CON (DRA=DRA1)
539
SIP INVITE:(A, Desde)
542
ISUP IAM: (CdPN=DRA1,CgPN=Desde)
545
ISUP ACM
548
ISUP ANM
551
SIP 100/180/183
554
SIP 200OK
557
SIP BYE
560
SIP 200OK
563
ISUP REL
569
ISUP RLC
575
SIP 200OK
572
A:
578
FIG. 7 (Llamada Contestada) O
FIG. 8 (Establecimiento de Llamada no Satisfactorio)

FIG. 5

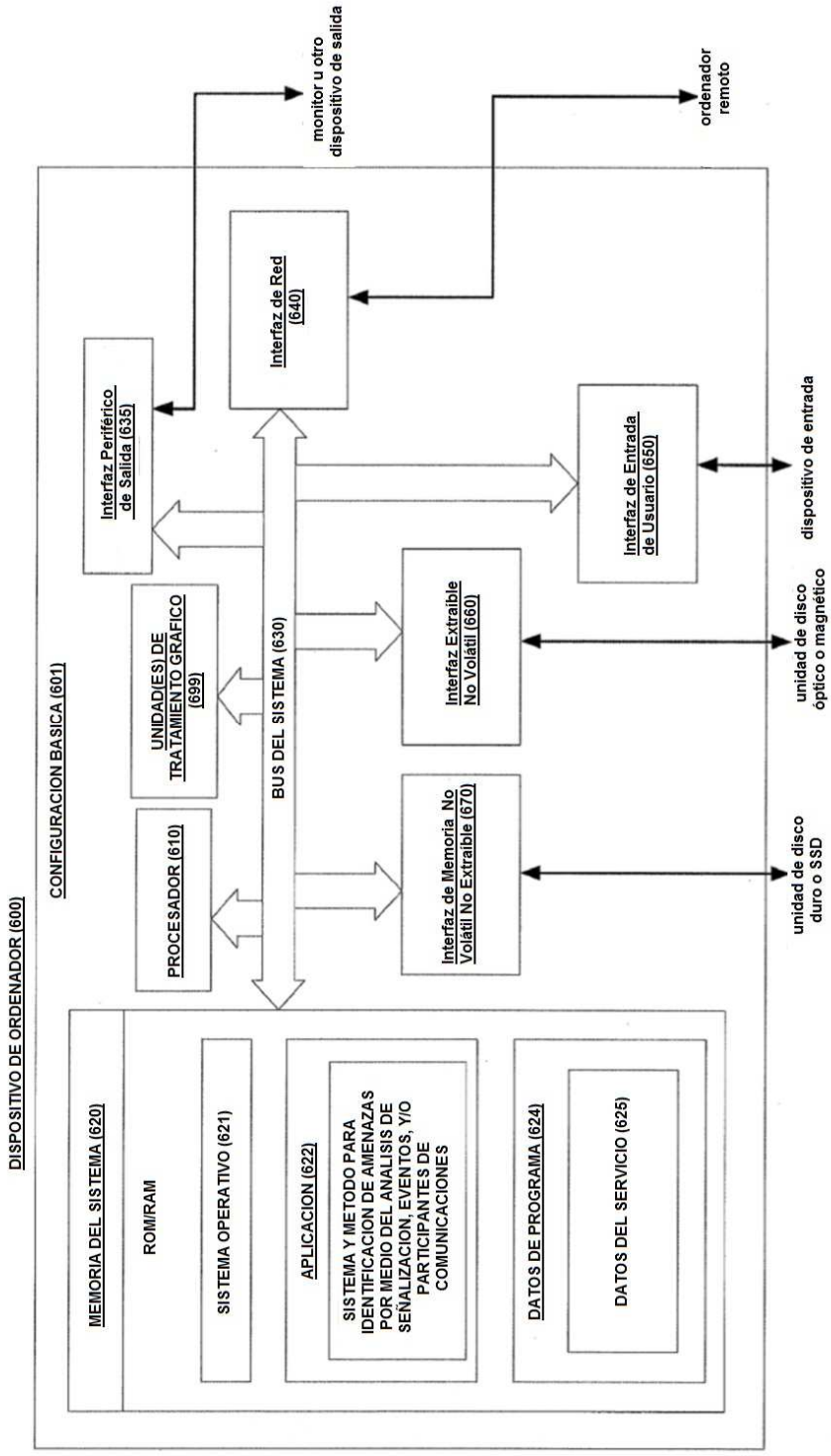

DISPOSITIVO DE ORDENADOR (600)
CONFIGURACION BASICA (601)
MEMORIA DEL SISTEMA (620)
ROM/RAM
SISTEMA OPERATIVO (621)
APLICACION (622)
SISTEMA Y METODO PARA IDENTIFICACION DE AMENAZAS POR MEDIO DEL ANALISIS DE SEÑALIZACION, EVENTOS, Y/O PARTICIPANTES DE COMUNICACIONES
DATOS DE PROGRAMA (624)
DATOS DEL SERVICIO (625)
PROCESADOR (610)
UNIDAD(ES) DE TRATAMIENTO GRAFICO (699)
BUS DEL SISTEMA (630)
Interfaz Periférico de Salida (635)
Interfaz de Red (640)
Interfaz de Entrada de Usuario (650)
Interfaz Extraible No Volátil (660)
Interfaz de Memoria No Volátil No Extraible (670)
monitor u otro dispositivo de salida
ordenador remoto
dispositivo de entrada
unidad de disco óptico o magnético
unidad de disco duro o SSD

FIG. 6

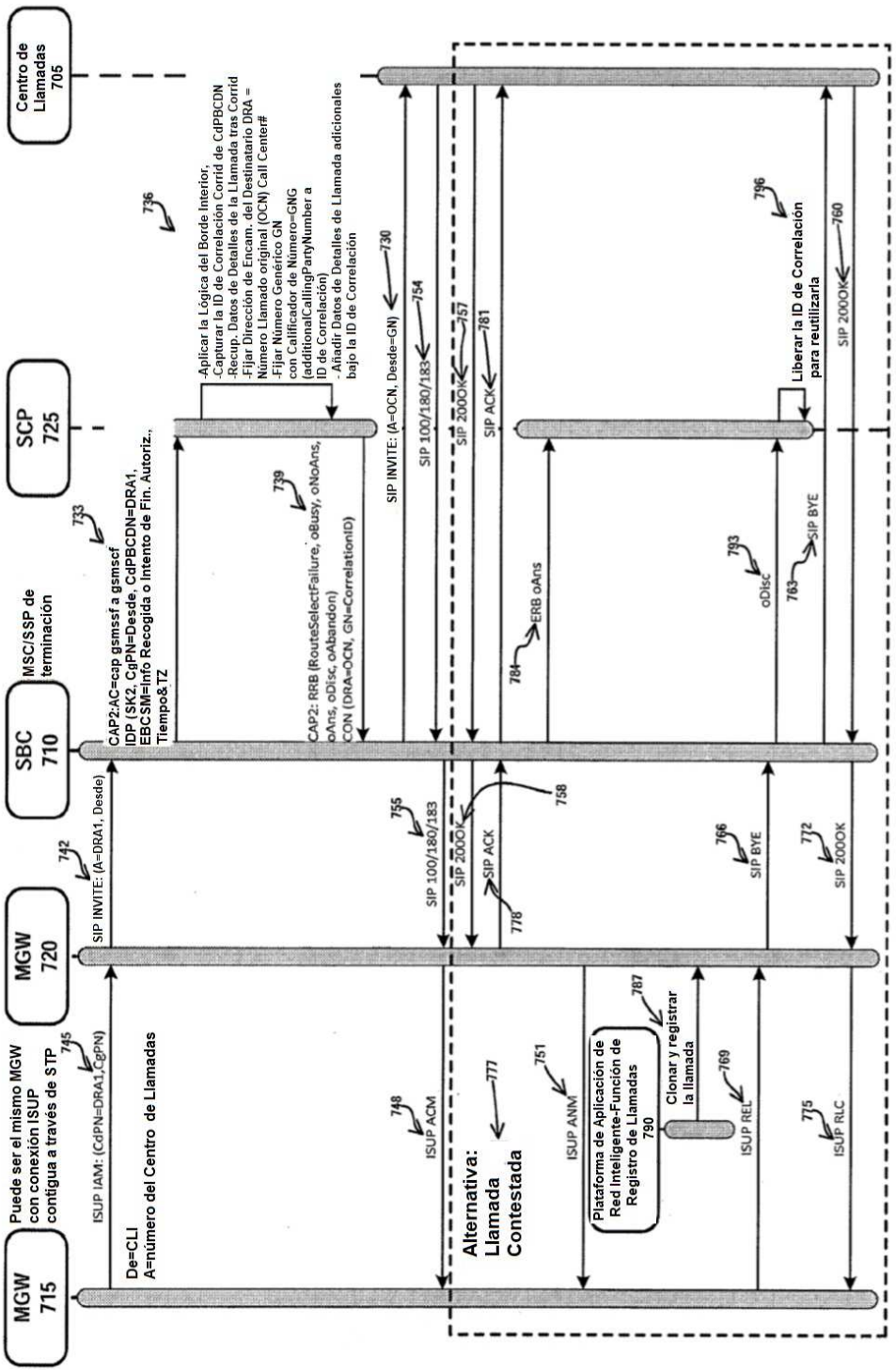

MGW 715
Puede ser el mismo MGW con conexión ISUP contigua a través de STP
MGW 720
SBC 710
MSC/SSP de terminación
SCP 725
Centro de Llamadas 705
ISUP IAM: (CdPN=DRA1,CgPN)
De=CLI
A=número del Centro de Llamadas
SIP INVITE: (A=DRA1, Desde)
CAP2:AC=cap gsmssf a gsmscf
IDP (SK2, CgPN=Desde, CdPBCDN=DRA1,
EBC:SM=info Recogida o Intento de Fin. Autoriz.,
Tiempo&TZ
-Aplicar la Lógica del Borde Interior,
-Capturar la ID de Correlación Corrid de CdPBCDN
-Recup. Datos de Detalles de la Llamada tras Corrid
-Fijar Dirección de Encam. del Destinatario DRA =
Número Llamado original (OCN) Call Center#
-Fijar Número Genérico GN
con Calificador de Número=GNG
(additionalCallingPartyNumber a
ID de Correlación)
- Añadir Datos de Detalles de Llamada adicionales
bajo la ID de Correlación
CAP2: RRB (RouteSelectFailure, oBusy, oNoAns,
oAns, oDisc, oAbandon)
CON (DRA=OCN, GN=CorrelationID)
SIP INVITE: (A=OCN, Desde=GN)
SIP 100/180/183
SIP 2000K
SIP ACK
ERB oAns
oDisc
SIP BYE
Liberar la ID de Correlación para reutilizarla
SIP 2000K
SIP 100/180/183
SIP 2000K
SIP ACK
SIP BYE
SIP 2000K
ISUP ACM
ISUP ANM
Plataforma de Aplicación de Red Inteligente-Función de Registro de Llamadas 790
Clonar y registrar la llamada
ISUP REL
ISUP RLC
Alternativa:
Llamada Contestada
736
733
739
730
754
757
781
784
793
783
796
760
755
758
778
766
772
745
742
748
777
751
787
769
775

FIG. 7

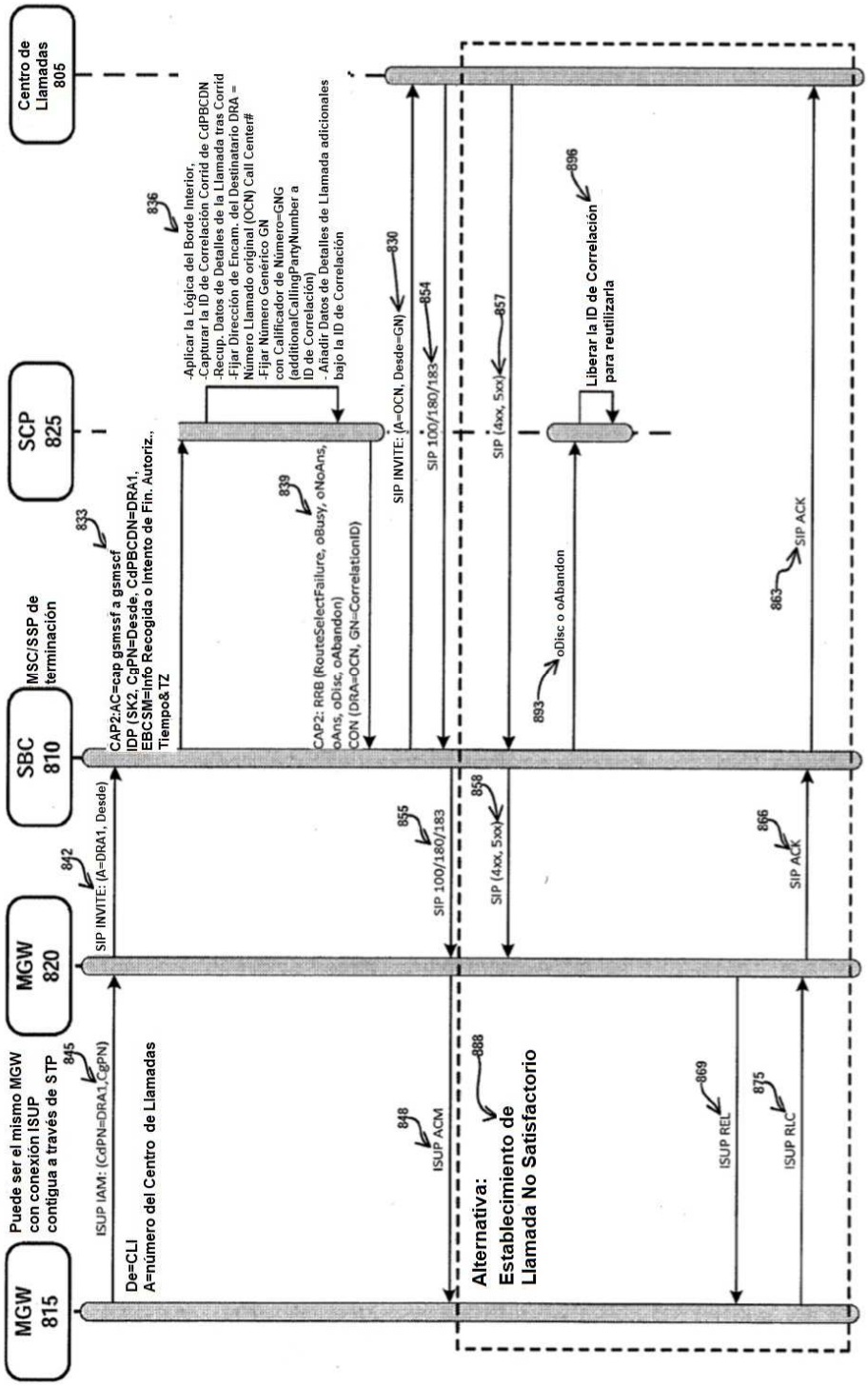
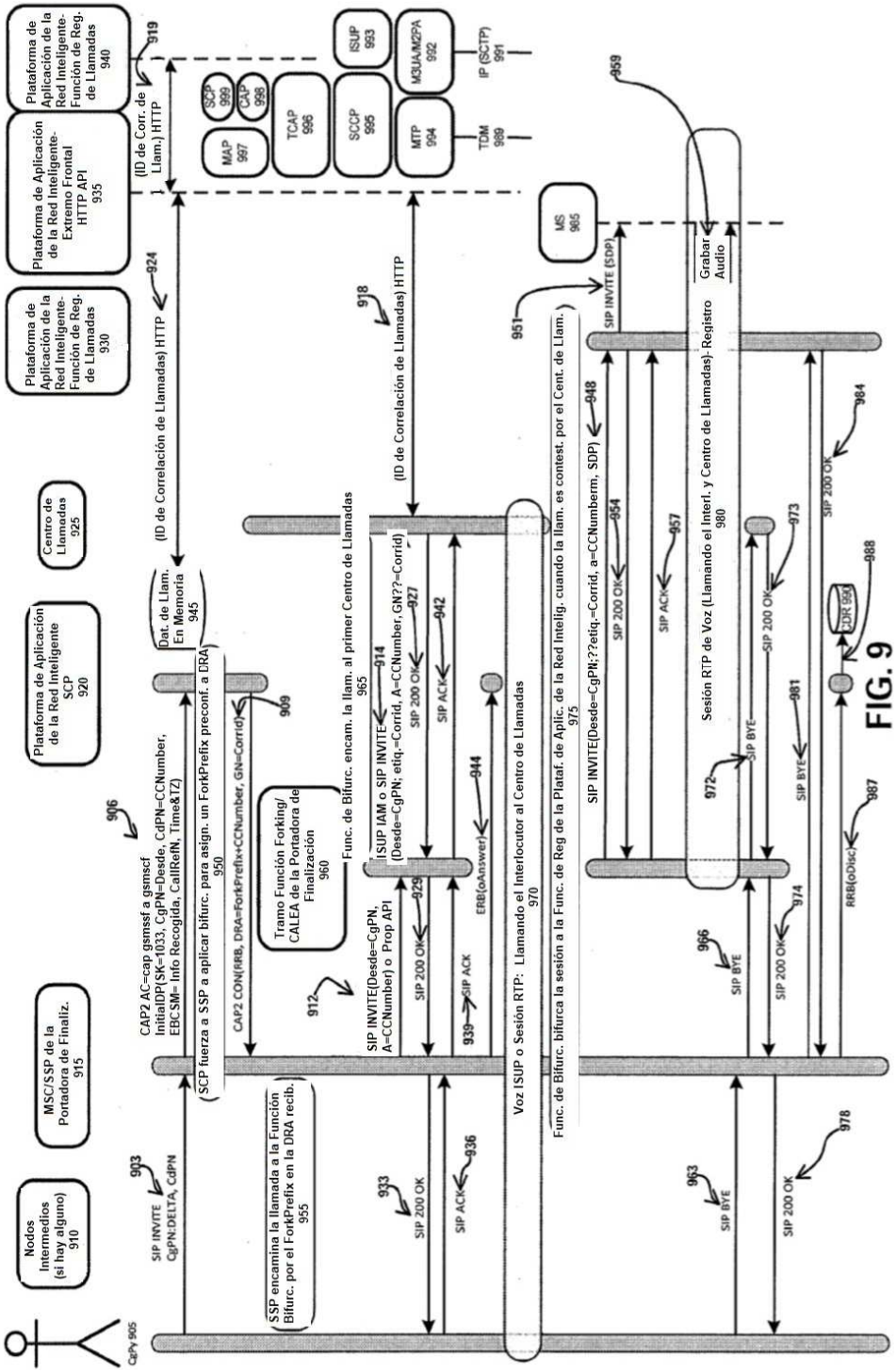

MGW 815
Puede ser el mismo MGW con conexión ISUP contigua a través de STP
MGW 820
SBC 810
MSC/SSP de terminación
SCP 825
Centro de Llamadas 805
ISUP IAM: (CdPN=DRA1,CgPN)
De=CLI
A=número del Centro de Llamadas
SIP INVITE: (A=DRA1, Desde)
CAP2:AC=cap gsmssf a gsmscf
IDP (SK2, CgPN=Desde, CdPBCDN=DRA1,
EBCSM=Info Recogida o Intento de Fin. Autoriz.,
Tiempo&TZ
-Aplicar la Lógica del Borde Interior;
-Capturar la ID de Correlación Corrid de CdPBCDN
-Recup. Datos de Detalles de la Llamada tras Corrid
-Fijar Dirección de Encam. del Destinatario DRA =
Número Llamado original (OCN) Call Center#
-Fijar Número Genérico GN
con Calificador de Número=GNG
(additionalCallingPartyNumber a
ID de Correlación)
- Añadir Datos de Detalles de Llamada adicionales
bajo la ID de Correlación
CAP2: RRB (RouteSelectFailure, oBusy, oNoAns,
oAns, oDisc, oAbandon)
CON (DRA=OCN, GN=CorrelationID)
SIP INVITE: (A=OCN, Desde=GN)
SIP 100/180/183
SIP (4xx, 5xx)
Liberar la ID de Correlación
para reutilizarla
oDisc o oAbandon
SIP ACK
SIP 100/180/183
SIP (4xx, 5xx)
SIP ACK
ISUP ACM
Alternativa:
Establecimiento de
Llamada No Satisfactorio
ISUP REL
ISUP RLC
842
845
833
836
839
830
854
857
896
893
863
855
858
866
848
888
869
875

FIG. 8


Plataforma de Aplicación de la Red Inteligente-Función de Reg. de Llamadas 940
Plataforma de Aplicación de la Red Inteligente-Extremo Frontal HTTP API 935
Plataforma de Aplicación de la Red Inteligente-Función de Reg. de Llamadas 930
Plataforma de Aplicación de la Red Inteligente SCP 920
Centro de Llamadas 925
Nodos Intermedios (si hay alguno) 910
MSC/SSP de la Portadora de Finaliz. 915
CgPy 905
(ID de Corr. de Llam.) HTTP
SCP 999
CAP 998
MAP 997
TCAP 996
SCCP 995
MTP 994
TDM 989
ISUP 993
M3UA/M2PA 992
IP (SCTP) 991
MS 965
(ID de Correlación de Llamadas) HTTP
Dat. de Llam. En Memoria 945
CAP2 AC=cap gsmssf a gsmscf InitialDP(SK=1033, CgPN=Desde, CdPN=CCNumber, EBC:SM= Info Recogida, CallRefN, Time&TZ)
(SCP fuerza a SSP a aplicar bifurc. para asign. un ForkPrefix preconf. a DRA)
CAP2 CON(ERB, DRA=ForkPrefix+CCNumber, GN=Corrid)
Trano Función Forking/ CALEA de la Portadora de Finalización
Func. de Bifurc. encam. la llam. al primer Centro de Llamadas
SIP INVITE CgPN:DELTA, CdPN
SSP encamina la llamada a la Función Bifurc. por el ForkPrefix en la DRA recib.
SIP INVITE[Desde=CgPN, A=CCNumber) o Prop API
ISUP IAM o SIP INVITE (Desde=CgPN; etiq.=Corrid, A=CCNumber, GN??=Corrid)
SIP 200 OK
SIP ACK
ERB(oAnswer)
Voz ISUP o Sesión RTP: Llamando el Interlocutor al Centro de Llamadas
Func. de Bifurc. bifurca la sesión a la Func. de Reg de la Plataf. de Aplic. de la Red Intelig. cuando la llam. es contest. por el Cent. de Llam.
SIP INVITE[Desde=CgPN;?etiq.=Corrid, a=CCNumberm, SDP)
SIP INVITE (SDP)
Grabar Audio
Sesión RTP de Voz (Llamando el Interl. y Centro de Llamadas)-Registro
SIP BYE
RRB(oDisc)
FIG. 9

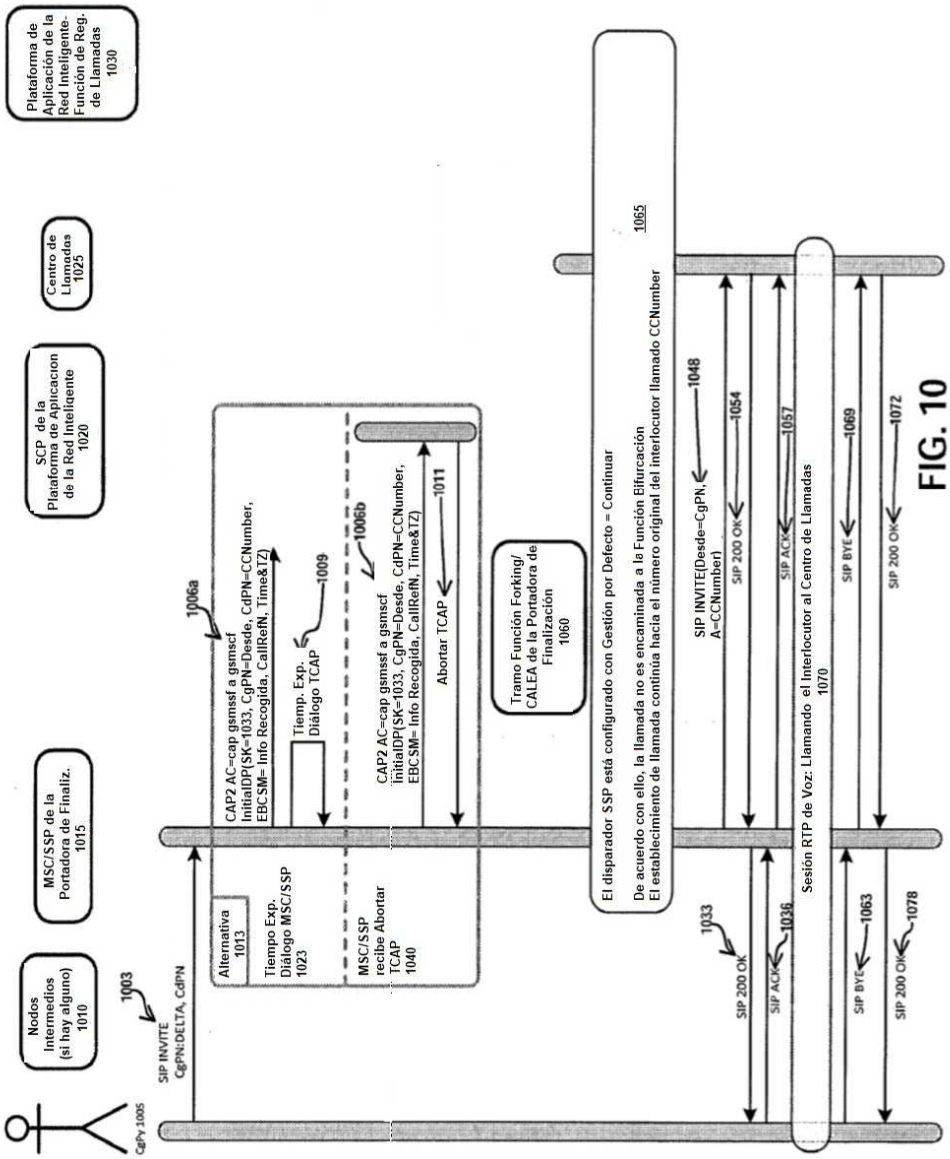

Plataforma de Aplicación de la Red Inteligente-Función de Reg. de Llamadas 1030
Centro de Llamadas 1025
SCP de la Plataforma de Aplicacion de la Red Inteligente 1020
MSC/SSP de la Portadora de Finaliz. 1015
Nodos Intermedios (si hay alguno) 1010
CgPy 1005
1003
SIP INVITE CgPN:DELTA, CdPN
1006a
CAP2 AC=cap gsmssf a gsmscf InitialDP(SK=1033, CgPN=Desde, CdPN=CCNumber, EBCSM= Info Recogida, CallRefN, Time&TZ)
Alternativa 1013
Tiempo Exp. Dialogo MSC/SSP 1023
Tiemp. Exp. Diálogo TCAP
1009
1006b
CAP2 AC=cap gsmssf a gsmscf InitialDP(SK=1033, CgPN=Desde, CdPN=CCNumber, EBCSM= Info Recogida, CallRefN, Time&TZ)
MSC/SSP recibe Abortar TCAP 1040
Abortar TCAP
1011
Tramo Función Forking/ CALEA de la Portadora de Finalización 1060
El disparador SSP está configurado con Gestión por Defecto = Continuar
De acuerdo con ello, la llamada no es encaminada a la Función Bifurcación
El establecimiento de llamada continúa hacia el número original del interlocutor llamado CCNumber
1065
SIP INVITE(Desde=CgPN, A=CCNumber)
1048
SIP 200 OK
1054
SIP ACK
1057
Sesión RTP de Voz: Llamando el Interlocutor al Centro de Llamadas 1070
SIP BYE
1069
SIP 200 OK
1072
1033
SIP 200 OK
SIP ACK
1036
SIP BYE
1063
SIP 200 OK
1078

FIG. 10

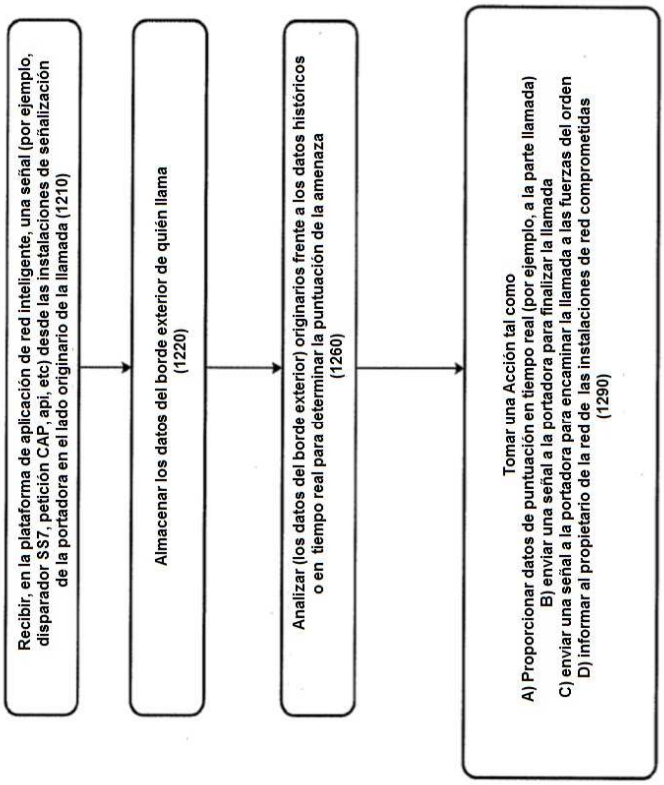

Recibir, en la plataforma de aplicación de red inteligente, una señal (por ejemplo, disparador SS7, petición CAP, api, etc) desde las instalaciones de señalización de la portadora en el lado originario de la llamada (1210)
Almacenar los datos del borde exterior de quién llama (1220)
Analizar (los datos del borde exterior) originarios frente a los datos históricos o en tiempo real para determinar la puntuación de la amenaza (1260)
Tomar una Acción tal como
A) Proporcionar datos de puntuación en tiempo real (por ejemplo, a la parte llamada)
B) enviar una señal a la portadora para finalizar la llamada
C) enviar una señal a la portadora para encaminar la llamada a las fuerzas del orden
D) informar al propietario de la red de las instalaciones de red comprometidas (1290)

FIG. 11a

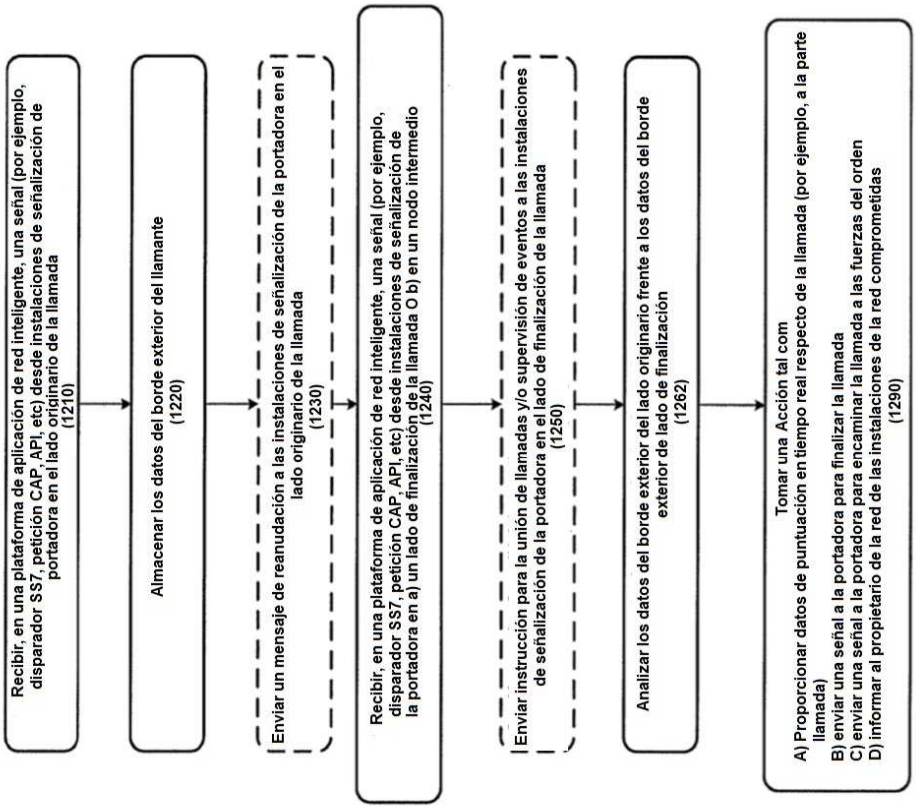

Recibir, en una plataforma de aplicación de red inteligente, una señal (por ejemplo, disparador SS7, petición CAP, API, etc) desde instalaciones de señalización de portadora en el lado originario de la llamada (1210)
Almacenar los datos del borde exterior del llamante (1220)
Enviar un mensaje de reanudación a las instalaciones de señalización de la portadora en el lado originario de la llamada (1230)
Recibir, en una plataforma de aplicación de red inteligente, una señal (por ejemplo, disparador SS7, petición CAP, API, etc) desde instalaciones de señalización de la portadora en a) un lado de finalización de la llamada O b) en un nodo intermedio (1240)
Enviar instrucción para la unión de llamadas y/o supervisión de eventos a las instalaciones de señalización de la portadora en el lado de finalización de la llamada (1250)
Analizar los datos del borde exterior del lado originario frente a los datos del borde exterior de lado de finalización (1262)
Tomar una Acción tal com
A) Proporcionar datos de puntuación en tiempo real respecto de la llamada (por ejemplo, a la parte llamada)
B) enviar una señal a la portadora para finalizar la llamada
C) enviar una señal a la portadora para encaminar la llamada a las fuerzas del orden
D) informar al propietario de la red de las instalaciones de la red comprometidas (1290)

FIG. 11b

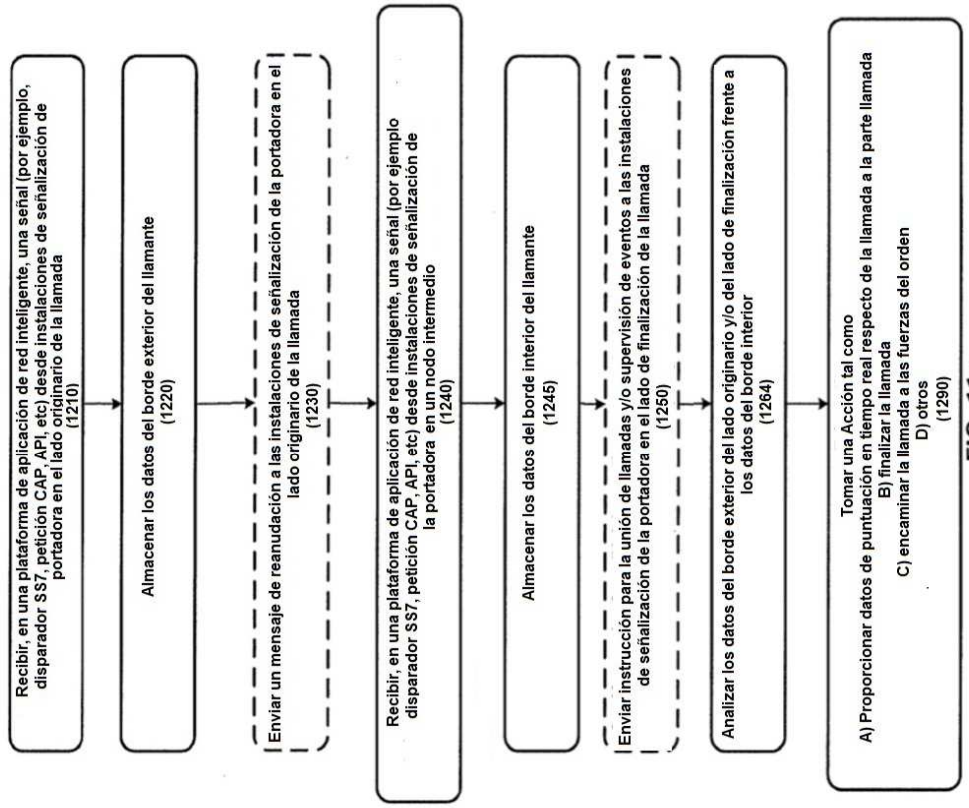

Recibir, en una plataforma de aplicación de red inteligente, una señal (por ejemplo, disparador SS7, petición CAP, API, etc) desde instalaciones de señalización de portadora en el lado originario de la llamada (1210)
Almacenar los datos del borde exterior del llamante (1220)
Enviar un mensaje de reanudación a las instalaciones de señalización de la portadora en el lado originario de la llamada (1230)
Recibir, en una plataforma de aplicación de red inteligente, una señal (por ejemplo disparador SS7, petición CAP, API, etc) desde instalaciones de señalización de la portadora en un nodo intermedio (1240)
Almacenar los datos del borde interior del llamante (1245)
Enviar instrucción para la unión de llamadas y/o supervisión de eventos a las instalaciones de señalización de la portadora en el lado de finalización de la llamada (1250)
Analizar los datos del borde exterior del lado originario y/o del lado de finalización frente a los datos del borde interior (1264)
Tomar una Acción tal como
A) Proporcionar datos de puntuación en tiempo real respecto de la llamada a la parte llamada
B) finalizar la llamada
C) encaminar la llamada a las fuerzas del orden
D) otros
(1290)

FIG. 11c

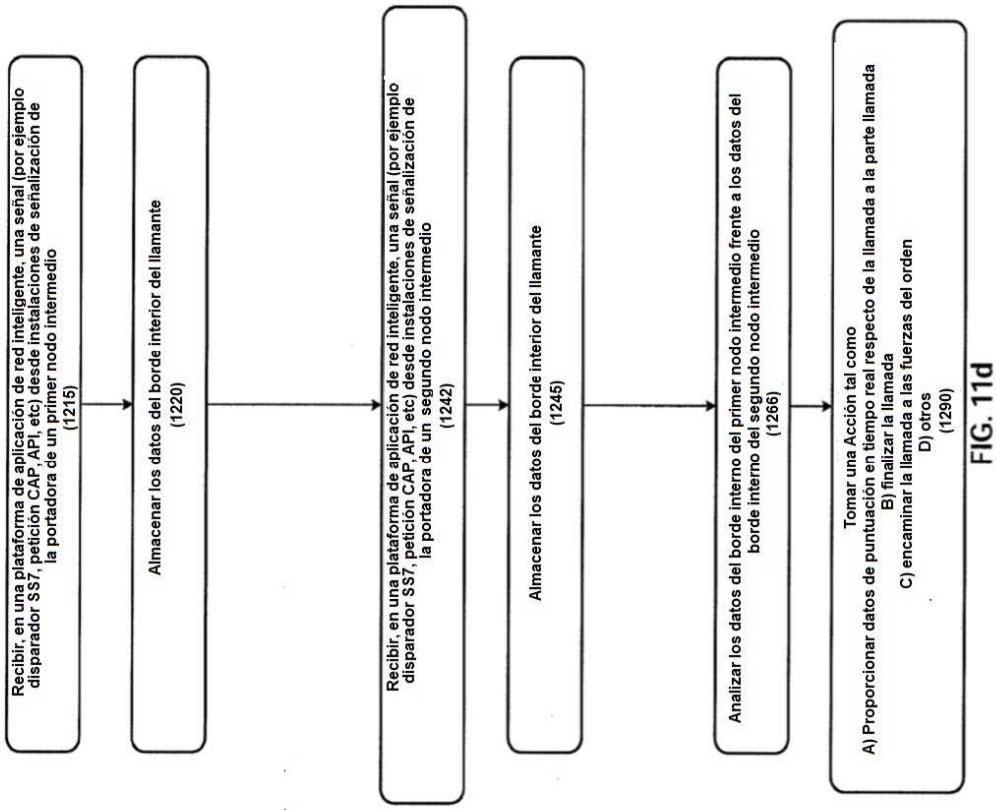

Recibir, en una plataforma de aplicación de red inteligente, una señal (por ejemplo disparador SS7, petición CAP, API, etc) desde instalaciones de señalización de la portadora de un primer nodo intermedio
(1215)
Almacenar los datos del borde interior del llamante
(1220)
Recibir, en una plataforma de aplicación de red inteligente, una señal (por ejemplo disparador SS7, petición CAP, API, etc) desde instalaciones de señalización de la portadora de un segundo nodo intermedio
(1242)
Almacenar los datos del borde interior del llamante
(1245)
Analizar los datos del borde interno del primer nodo intermedio frente a los datos del borde interno del segundo nodo intermedio
(1266)
Tomar una Acción tal como
A) Proporcionar datos de puntuación en tiempo real respecto de la llamada a la parte llamada
B) finalizar la llamada
C) encaminar la llamada a las fuerzas del orden
D) otros
(1290)

FIG. 11d

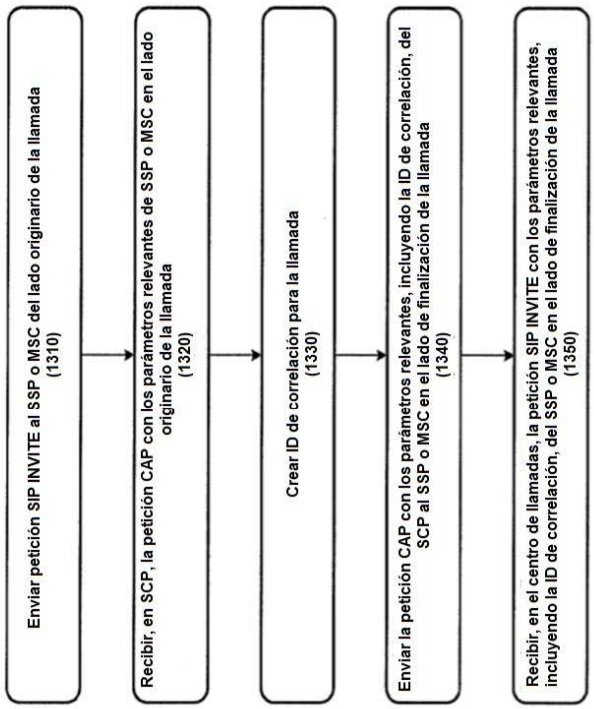

Enviar petición SIP INVITE al SSP o MSC del lado originario de la llamada (1310)
Recibir, en SCP, la petición CAP con los parámetros relevantes de SSP o MSC en el lado originario de la llamada (1320)
Crear ID de correlación para la llamada (1330)
Enviar la petición CAP con los parámetros relevantes, incluyendo la ID de correlación, del SCP al SSP o MSC en el lado de finalización de la llamada (1340)
Recibir, en el centro de llamadas, la petición SIP INVITE con los parámetros relevantes, incluyendo la ID de correlación, del SSP o MSC en el lado de finalización de la llamada (1350)

FIG. 12